7275
AES-*Network Management System* (NMS)

User Manual

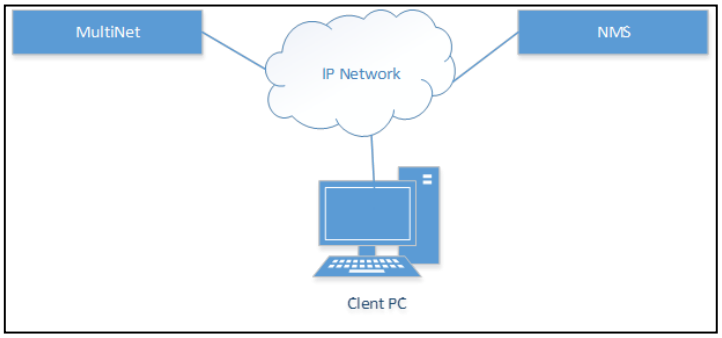
Table of Contents

1 Product Overview 4
1.1 NMS Product Description 4
1.1.1 Multi-level Intelligent Network Dashboards 4
1.1.2 Interactive Radio Network Visualization 5
1.1.3 24/7 Notification 5
1.2 NMS Server Specifications 6
1.3 NMS Software and Hardware Requirements 6
2 Installation and Configuration 7
2.1 Installation Preparation 7
2.1.1 NMS Server 7
2.1.2 AES-*MultiNet* Receiver 7
2.2 Connect and Power up NMS Server 7
2.3 Access the Administrator Dashboard 8
2.3.1 Enter Contact Information 8
2.3.2 Configure the NMS Server IP settings 8
2.3.3 Enter AES-*MultiNet* Receiver parameters 8
2.3.4 Verify that the NMS is communicating with the AES-*MultiNet* Receiver 9
3 System Operation Summary 10
4 Administrator Dashboard 11
4.1 Administrator Dashboard - Status 11
4.2 NMS Server Configuration 12
4.2.1 AES-*MultiNet* Receiver Configuration 12
4.2.2 External Name Configuration 12
4.3 System Maintenance 13
4.3.1 Passwords 13
4.3.2 Contact Section 14
4.3.3 License Section 14
4.4 Operator Operations 15
5 Operator Dashboard 16
5.1 Overview 16
5.2 IP Link and Subscriber Status Monitoring 17
5.2.1 IP Link Status Monitoring 17
5.2.2 Subscriber Status Monitoring 17
5.2.3 View Fault List – Fault Detail Windows 17
5.3 Network Health Score 18
5.4 Network Pulse 19
5.5 Network Analysis Tools 19
5.5.1 IP Links – Load 20
5.5.2 Subscribers – Top Talkers 21
5.5.3 Subscribers – Top Repeaters 22
5.5.4 Subscribers – Late Check-Ins 22
5.5.5 Subscribers – Frequent Check-Ins 23
5.5.6 Mesh – Hops 23

5.5.7 Mesh – Ack Delays 24
5.5.8 Mesh – NetCon 24
5.6 Equipment List 25
5.6.1 Equipment List - IP Links 25
5.6.2 Equipment List - Subscribers 26
5.7 Maintenance – Operator Dashboard 28
6 Interactive Visualization 29
6.1 Overview 29
6.2 Enter Subscriber and IP Link Addresses into NMS 29
6.3 Launch Interactive Visualization 29
6.4 Utilization View 31
6.5 Faults View 32
6.6 Mesh Topology View 33
6.7 Routes View 35
7 Notification 37
7.1 Notification Set-up 37
7.2 Recipients 37
7.3 Triggers 38
7.4 Associations 39
8 Warranty 41

1 Product Overview

The AES-*Network Management System* (NMS) is a complete end-to-end AES-*IntelliNet* mesh radio network monitoring and management platform. NMS provides a real-time visual presentation of the operation and function of an AES-*IntelliNet* network. The NMS platform can also drive down overall network management costs while supporting efficient and profitable network growth as additional AES-*IntelliNet* subscribers are deployed. NMS monitors all network subsystems which includes AES-*MultiNet* receivers, IP Links, Burglary and Fire Subscribers and delivers real-time notifications of system events.



NOTE: Closely follow the entire contents of this User Manual as it contains information that is essential to successfully completing the proper installation of the 7275 AES-*Network Management System* (NMS).

1.1 NMS Product Description

This release of NMS offers the following features:

- Multi-level Intelligent Network Dashboards
- Radio Network Interactive Visualization of each Business Unit
- 24/7 Notifications via email or SMS of network events to key personnel

1.1.1 Multi-level Intelligent Network Dashboards

NMS features multi-level browser based dashboard architecture for system configuration, maintenance, and operation. The *Administrator Dashboard* is designed for the AES-*MultiNe*t owner and provides real-time status of AES-*MultiNet* connectivity and the NMS server once the system is set up and operating. Through the *Administrator Dashboard*, the AES-*MultiNet* owner sets up and supports:

- Configuration of AES-*MultiNet* receiver parameters
- Configuration of NMS server parameters
- Edit User credentials for access to the *Operator Dashboards* – one for each Business Unit
- Remote software upgrade of NMS server
- Reset to factory defaults for NMS server
- Overall appliance Status

Each AES-*MultiNet* Business Unit is set up with a separate *Operator Dashboard* that provides visibility into radio signal traffic and overall operation. This dashboard displays critical Business Unit information in a dynamic and intuitive format to enable a quick assessment of the network's performance and to quickly identify events that could affect network operation. For example, the *Network Pulse* dynamically tracks key performance indicators including subscriber Check-ins and Ack Delays over the most recent ten day period. The *Network Health Score* quantifies overall network operational quality on a scale between 0 - 100.

Below is a list of Business Unit specific data displayed in a user-friendly format on the *Operator Dashboard:*

- List of Subscribers needing service
- List of IP Links needing service
- Network performance charts
- Total received packets
- IP Link Load
- List of Top Talking Subscribers
- List of Top Repeater Subscribers
- List of Subscribers with Late Check-ins
- List of Subscribers with Check-ins more than once per 24 hrs.
- List of Subscribers with high number of Hops
- List of Subscribers sending Acknowledgement (Ack) Delay signals
- List of Subscribers sending a NetCon signal
- IP Link Equipment List
- Subscriber Equipment List
- Link for Google Earth™ for interactive visualization of network

1.1.2 Interactive Radio Network Visualization

Radio Network Visualization is a feature accessed through the *Operator Dashboards* that presents an interactive geographical layout of the AES-*IntelliNet* network using Google Earth. It will show Business Unit specific information such as the following:

- Subscriber positions
- Subscriber status
- IP Link positions
- IP Link status
- Most Used Route
- Most Recent Route
- Route and distance information
- Subscribers requiring service
- IP Links requiring service
- Subscriber utilization
- IP Link utilization

1.1.3 24/7 Notification

The Notification function enables users to monitor their AES-*IntelliNet* network from anyplace at any time. Through the *Operator Dashboard*, users can configure automatic alerts based on the system-wide *Network Health Score* to send alerts by both SMS and email to key personnel. Triggers can also be set up for alerts due to many types of subsystem faults with any Subscriber or IP Links. The user can create the list of personnel to be notified, define the fault criteria to be reported, and create associations between the alerts and personnel to optimize responses.

1.2 NMS Server Specifications

Server Appliance Hardware Specifications
The NMS is a rack mountable 1U network appliance that runs on an Intel Atom D2550 processor. It features an Intel NM10 chipset and board based on HB131. This security appliance also includes 2x GbE Ethernet, 2x SATA 3 Gb/s, 1x mSATA option, DDR3 So-DIMM, up to 4GB system memory, 240GB of Solid State Storage.

Server Appliance Software Specifications
Dashboard, Visualization, and Notification applications are implemented over an industry standard Linux environment.

1.3 NMS Software and Hardware Requirements

- Client PC for accessing NMS *Administrator Dashboard* and Google Earth™
  - Google Earth application
  - Internet access for Google Earth during operation
  - Network Access for NMS Dashboard
  - Internet Browser such as Internet Explorer 10 or newer, Firefox, Chrome etc.
- NMS Server (Included with NMS)
- NMS Server Ethernet cable (Included with NMS)
- NMS Server AC power cord (Included with NMS)
- Uninterrupted Power Supply
- AES-*MultiNet* must have Version 467 or later installed. When connected to a MN 467, NetCon faults will not be shown

2 Installation and Configuration

2.1 Installation Preparation

It is recommended to collect all configuration information prior to starting installation to reduce installation time.

2.1.1 NMS Server

Take a note of the NMS factory default addresses as they will be needed when connecting with the NMS Server for the first time:

1. Default IP: 192.168.1.254
2. Default NM: 255.255.255.0
3. Default GW: 192.168.1.1
4. Default DNS1: 8.8.8.8
5. Default DNS2: "blank"

The following information will be required for setting up the NMS Server with your preferred settings.

1. Private IP address
2. Subnet Mask
3. Default Gateway
4. DNS Server 1
5. DNS Server 2 (optional)
6. Public IP address (optional)
    a. TCP port 1194, 1195 for AES VPN

2.1.2 AES-*MultiNet* Receiver

Only one AES-*MultiNet* Receiver can be monitored at a time, so identify which AES-*MultiNet* (usually the Primary AES-*MultiNet*) is to be monitored by the NMS and collect the information below.

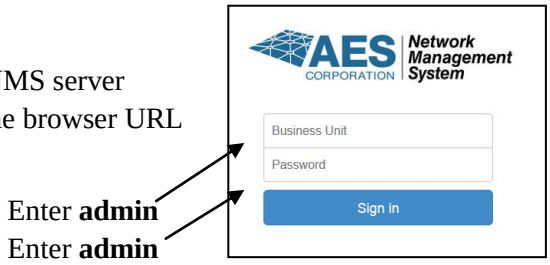
1. AES-*MultiNet* IP address
2. AES-*MultiNet* password

2.2 Connect and Power up NMS Server

1. Connect the power cord to NMS and plug into an outlet, NMS server will power up right away
2. Connect NMS Server (Ethernet port labeled 1) to an IP network or PC where it can be reached with the factory IP address (192.168.1.254) from a PC for configuration purposes

2.3 Access the Administrator Dashboard

1. Open a web browser on a PC on the same network as NMS server
2. Enter the default IP address: *https://192.168.1.254* in the browser URL
3. This will open the Administrator login screen
4. Login as Administrator
   Enter "admin" in Business Unit field and use the password "admin", note the password can be changed later

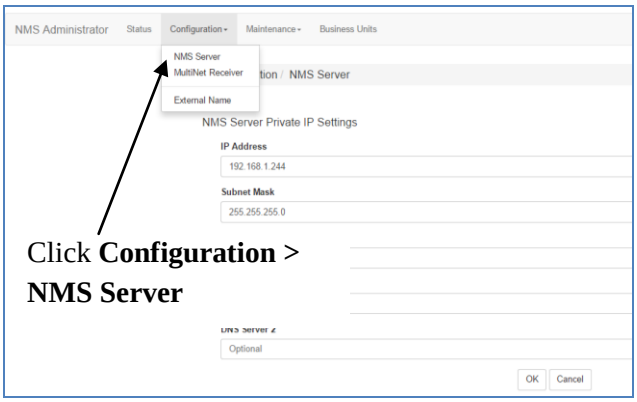


2.3.1 Enter Contact Information

1. Click on **Maintenance**
2. Then **Contact**
3. Enter contact information
4. Click **Save**

2.3.2 Configure the NMS Server IP settings

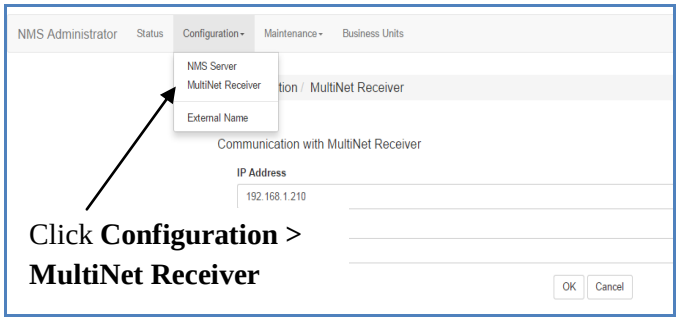
1. In the *Administrator Dashboard* click on **Configuration** > **NMS Server** to change the NMS IP settings
2. Change the NMS IP settings to the preferred network settings on the same network as AES-*MultiNet*
3. Click **OK**
4. Power down the NMS server by pushing and releasing the power button, the NMS will power down within 10 seconds



NMS Server IP Settings

2.3.3 Enter AES-*MultiNet* Receiver parameters

1. Disconnect NMS sever from the initial network if not the same IP network as the AES-*MultiNet* receiver
2. Move the server to the permanent rack location, use the rack mount brackets included
3. Connect server to same IP network as AES-*MultiNet* receiver (Ethernet port labeled 1)
4. Access the *Admin Dashboard*, enter new NMS IP address URL and same login as before (see Section 2.3)
5. Click on **Configuration** > **MultiNet Receiver**
6. Enter the AES-*MultiNet* receiver IP Address and password
7. Click **OK** and NMS will restart and begin

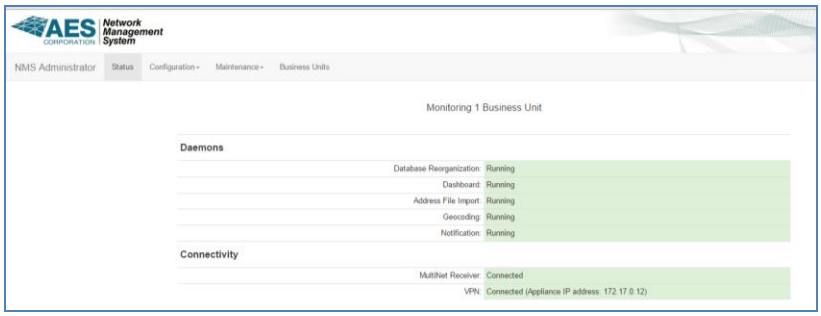


AES-*MultiNet* Receiver Parameters

2.3.4 Verify that the NMS is communicating with the AES-*MultiNet* receiver

1. After the NMS server restarts, access the *Administrator Dashboard* by entering the new IP address *https://new NMS IP address*
2. Within a few minutes, verify that you see the number of Business Units monitored at the top of the *Status* screen. The number might change as information is retrieved from the AES-*MultiNet*. This could take between 15 minutes and a few hours, depending upon the size of the database.

Please note, AES-*MultiNet* operation is never affected in any way by the operation of NMS.



Administrator Dashboard Status screen – Verify number of Business Units monitored.

Conclusion

The AES-*Network Management System* is now ready for operation. The next sections provide additional information and operational instructions.

3 System Operation Summary

NMS features multi-level browser based dashboard architecture for system configuration, management, and operation. The *Administrator Dashboard* is designed for the AES-*MultiNe*t receiver owner. The *Operator Dashboard* is designed for each Business Unit (one User per Business Unit). The *Administrator* and the *Operator Dashboards* can both be accessed at the URL for your NMS IP Address, but they have different capabilities and different login credentials. Below are some capabilities of the *Administrator* and *Operator Dashboards*.

Administrator Dashboard - Monitoring and Configuration Capabilities:

- NMS system and AES-*MultiNet* connectivity status
- NMS private and public IP settings
- Settings for communication with AES-*MultiNet*
- NMS factory reset and restart
- NMS software upgrade
- User credential configuration

Operator Dashboard Monitoring Capabilities:

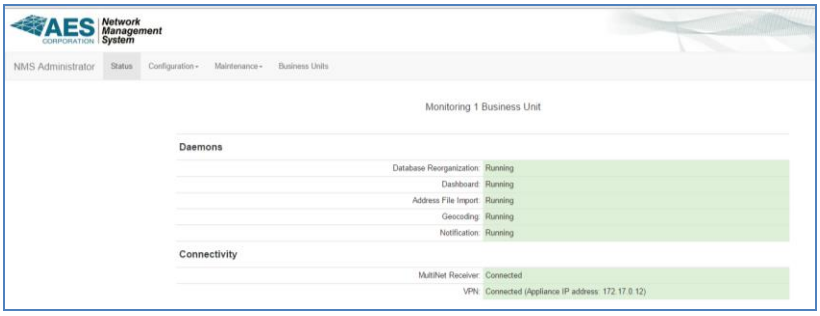
- Network Health Score
- Subscriber and IP Link service requirements
- Network Pulse
- IP Link load
- List Top Talker Subscribers
- List Top Repeater Subscribers
- List Late Check-in Subscribers
- List Frequent Check-in subscribers
- List Subscribers with 4 or more Hops
- List Subscribers with Ack Delays
- List Subscribers with NetCon trouble
- List of IP Links and Subscribers with model and revision numbers
- Subscriber and IP Link addresses import for Google Earth™
- Google Earth access
- Set up 24/7 Notifications or network events
- Operator password change

.

4 Administrator Dashboard

4.1 Administrator Dashboard - Status

See Section 2.3 for instructions on accessing the *Administrator Dashboard*. When first launched, the *Administrator Dashboard* displays the status of the AES-*MultiNet* receiver and the NMS server as detailed in the screen below followed by an explanation of each of the sections on the status screen. Click on **Status** to return to the *Status* screen.



Administrator Dashboard – Status Screen

Overview of Status Screen

Database Reorganization

Indicates proper optimization of databases and gathering of data from the AES-*MultiNe*t receiver and reorganizing in NMS

Dashboard

Indicates that Dashboard calculations and preparation of data for presentation on the Dashboards are operating properly

Address file Import

Indicates status of importing addresses from a .csv file in to the NMS

Geocoding

Indicates status of geocoding when finding GPS coordinates for the provided addresses

Notification

Indicates status of Notification function – NMS monitoring for trigger conditions configured by users

VPN

VPN for remote support from AES Tech Support team

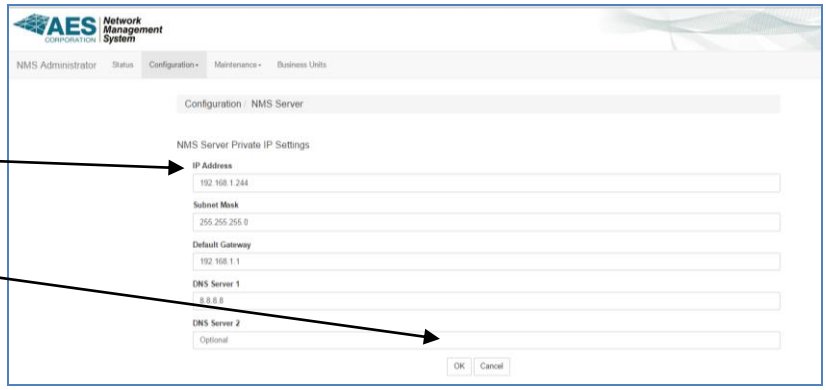
4.2 NMS Server Configuration

The view below will be displayed after clicking on **Configuration** then selecting **NMS Server**. This allows you to enter and change NMS private IP setting.

Click **Configuration>NMS Server**

Then enter NMS server IP settings

Then click **OK**



Configure NMS Server Screen

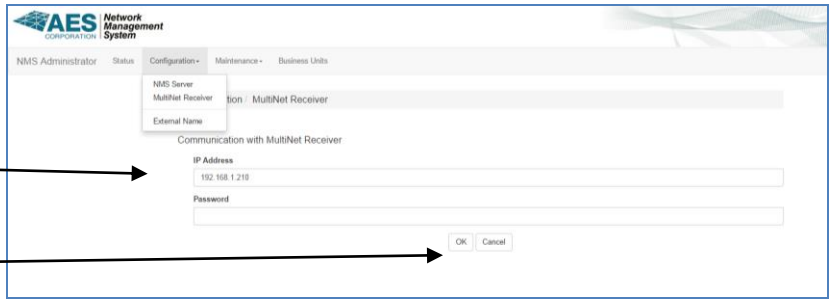
4.2.1 AES-*MultiNet* Receiver Configuration

The view below will be displayed after clicking on **Configuration** then selecting **MultiNet Receiver**. This allows you to change AES-*MultiNet* Receiver settings.

Click
Configuration > MultiNet Receiver

Then enter AES-*MultiNet* IP address and password

Then click **OK**



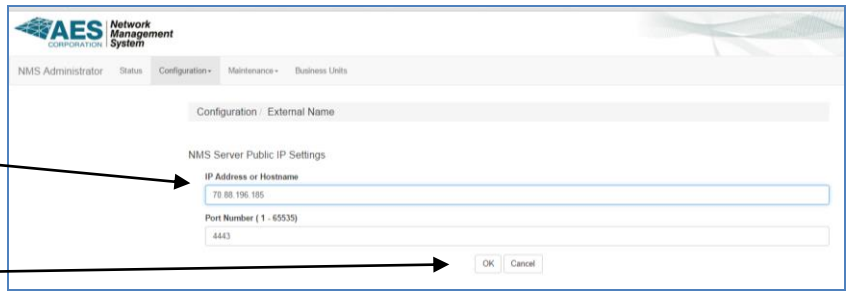
4.2.2 External Name Configuration

The view below will be displayed after clicking on **Configuration** then selecting **External Name**. This allows you to change NMS public IP settings for communication from outside the LAN.

Click
Configuration>External Name

Then enter a public IP address or host name and port number if needed for access from outside the LAN

Then click **OK**



4.3 System Maintenance

The view below will be displayed after clicking on **Maintenance** then selecting **System**. This allows you to do the following:

1. Restart the NMS server . When you click on **Restart** the NMS system will restart. If the NMS server is restarted, contact information, license information, and NMS server IP settings will not be affected.

2. Upgrade NMS software using an upgrade package or URL. The new upgrade package and passphrase will be provided by AES. Upgrading the NMS software will cause a restart to the NMS appliance.

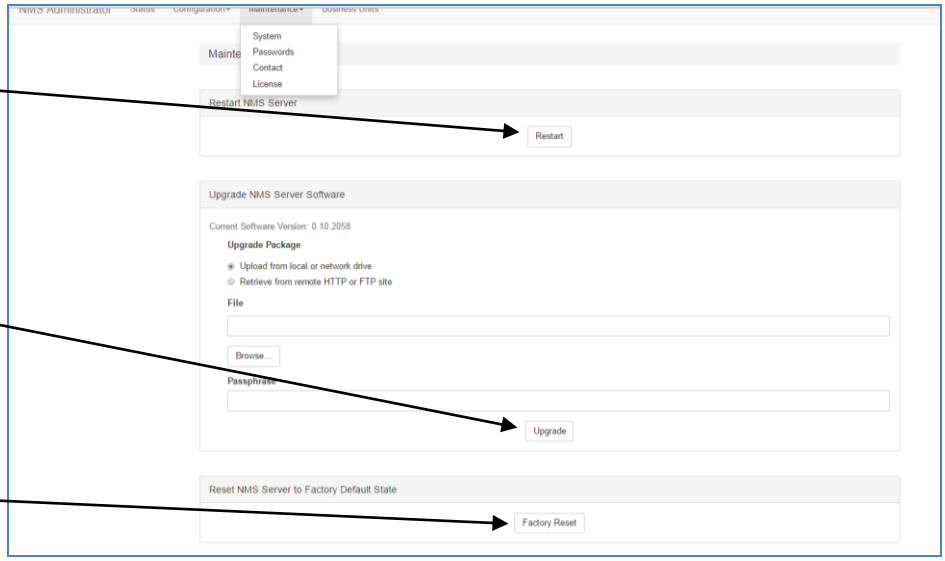
3. Reset NMS to Factory Default State. This action will reset the system to original status. All passwords will be reset to default sand all Business Unit data will be lost. The NMS IP address will not be lost. The NMS IP address is the only setting that is saved if NMS is reset to default state.

Click **Maintenance > System**

Next, click **Restart**

Upgrade NMS software: browse to select file and click Upgrade

Click here to **Reset** to Factory Default state



4.3.1 Passwords

The view below will be displayed after clicking on **Maintenance** then selecting **Password**. This allows you to set and/or change the *Administrator Dashboard* password as well as the *Operator Dashboard* passwords for all Business Units. The factory default log in and password for access to the *Operator Dashboard* at start up is *admin* (enter into Business Unit field – see section 2.3) and *admin* for password.

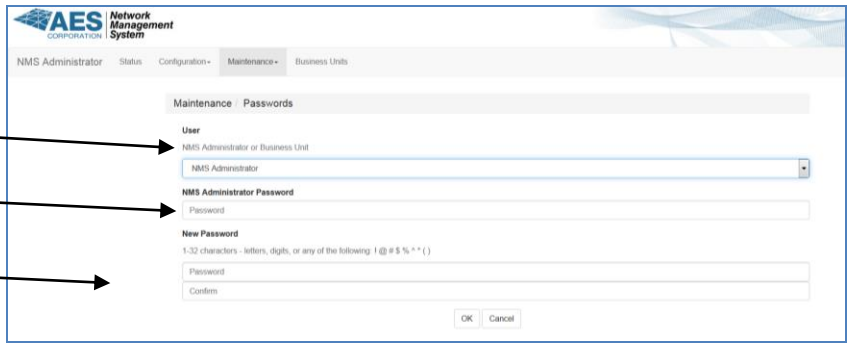
Click **Maintenance > Password**

Next, select either NMS Administrator or Business Unit

Then enter current Admin password

Then enter new Password twice

Click **OK** to save



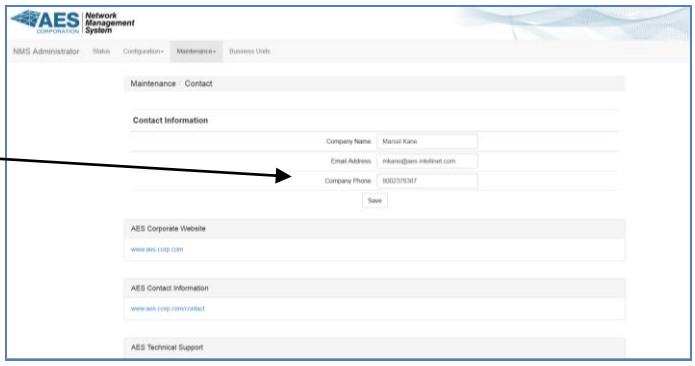
4.3.2 Contact Section

The view below will be displayed after clicking on **Maintenance** then selecting **Contact**. This screen allows the AES-*MultiNet* owners to input contact information. The contact section is not affected by a system restart.

Click **Maintenance > Contact** then

Enter Administrator contact information including email and phone

Then Click **Save**



Contact Section

4.3.3 License Section

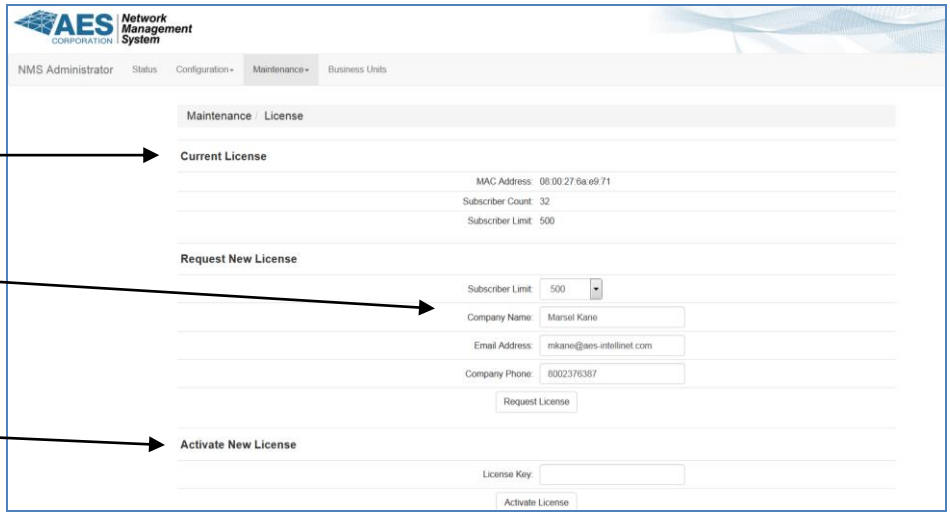
The view below will be displayed after clicking on **Maintenance** then selecting **License**. This is an important system wide view of the current license capacity of AES Subscribers supported by NMS software. Compare the Subscriber count to Subscriber limit to determine if a license update is needed. Use the **Request New License** section to initiate the process to update. Upon completion of the transaction, you will have a new license key which is entered into the **Activate New License** section to automatically update the license and capacity of Subscribers supported by NMS. The License section is not affected by a system restart.

Click **Maintenance > License**

Displays current License

Request a new license here

Activate new license with license key from AES here

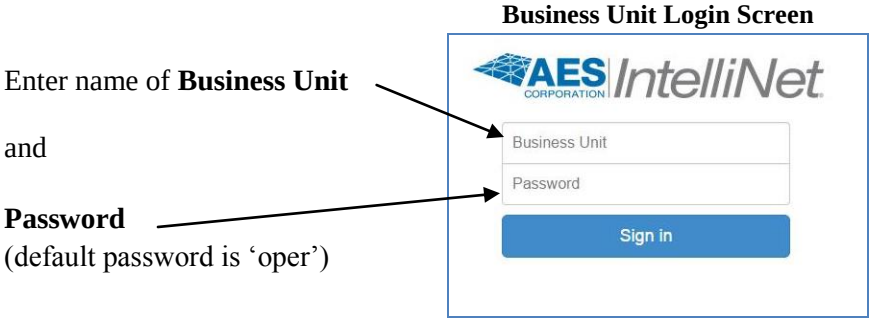


License Section

4.4 Operator Operations

If you are the AES-*MultiNet* owner and have access to the *Administrator Dashboard*, you can access the *Operator Dashboard* for any Business Unit by clicking on **Business Units** then click on any Business Unit listed. This will launch the *Operator Dashboard* for that Business Unit in a separate tab. The *Administrator Dashboard* remains open. The Administrator can open multiple Business Unit *Operator Dashboards*. If you are a Business Unit Owner, you can access your *Operator Dashboard* by signing in at your NMS IP Address URL to launch the login screen below. The username will be the AES-*MultiNet* Business Unit name and the initial password is "oper". Each Business Unit has its own username but the password is the same for all Business Units, "oper". This can be changed after login. Business Unit users should coordinate *Operator Dashboard* password management with the AES-*MultiNet* owner.

Business Unit Login Screen



5 Operator Dashboard

5.1 Overview

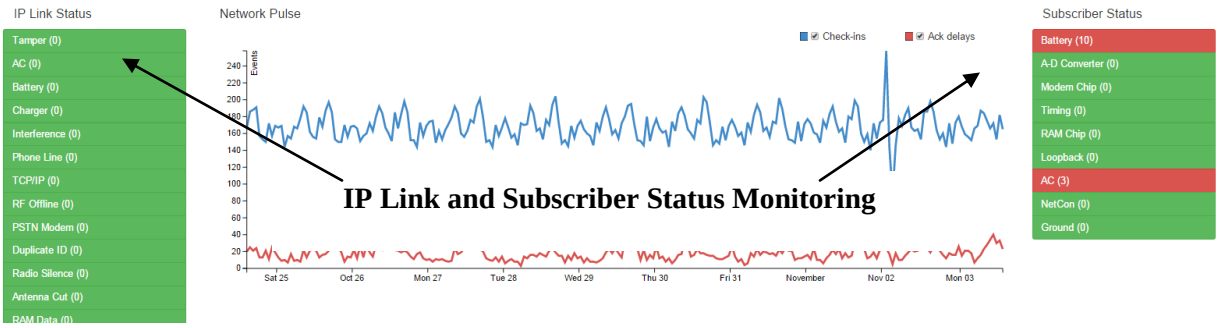
The *Operator Dashboard* displays all information available from the AES-*MultiNet* receiver for that Business Unit for the last 10 days. Each *Operator Dashboard* provides the following important information to the operator to help manage, monitor, and maintain the AES-*IntelliNet* network.

Operator Dashboard Monitoring Capabilities:

- Network Health Score
- Subscriber and IP Link service requirements
- Network Pulse
- IP Link load
- List Top Talker Subscribers
- List Top Repeater Subscribers
- List Late Check-in Subscribers
- List Frequent Check-in subscribers
- List Subscribers with 4 or more Hops
- List Subscribers with Ack Delays
- List Subscribers with NetCon trouble
- List of IP Links and Subscribers with model and revision numbers
- Subscriber and IP Link addresses import for Google Earth
- Google Earth access
- Set up 24/7 Notifications or network events
- Operator password change

5.2 IP Link and Subscriber Status Monitoring

If IP Link and Subscriber faults occur, these faults are highlighted on the left and right panels of the Dashboard to indicate new service requirements in real time do that they can be scheduled in the normal workflow. The green color indicates that there are no faults with any Subscribers or IP Links.



5.2.1 IP Link Status Monitoring

New IP Link faults will flash red-white for 10 seconds then remain red. These faults can flash again red-white when the browser is refreshed but if you click on any of the faults to view them, they will remain red.

5.2.2 Subscriber Status Monitoring

New Subscriber faults will flash orange-white for 10 seconds then stay orange. If a new Subscriber is added to a fault, the fault will flash red-white for 10 seconds then remain red.

5.2.3 View Fault List – Fault Detail Windows

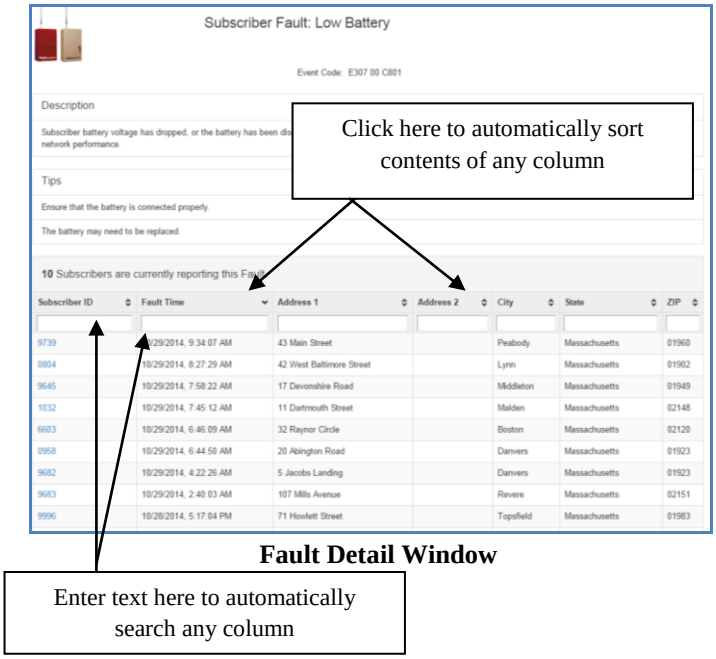
Each fault is described by name and in parentheses next to the name is the number of IP Links or Subscribers on the network experiencing that fault. To view a list of IP Link or Subscribers with the fault, click on the red button for that fault to open a Fault Detail Window. An example is below – a list of Subscribers with a low battery fault condition.

To access Fault Detail Window, Click on a fault. This is an example of Subscriber Battery Fault Detail Window – on right.ERE

The IP Link and Subscriber fault detail windows privide the following:

- Name of the fault and Event code
- A description of the fault and what causes it
- Tips for resolving this fault
- Total number of IP Links or Subscribers experiencing this fault
- Sortable list of IP Links or Subscribers experiencing this fault and the time stamp

Filters at the top of each column permit easy search and sort of the contents of the column.

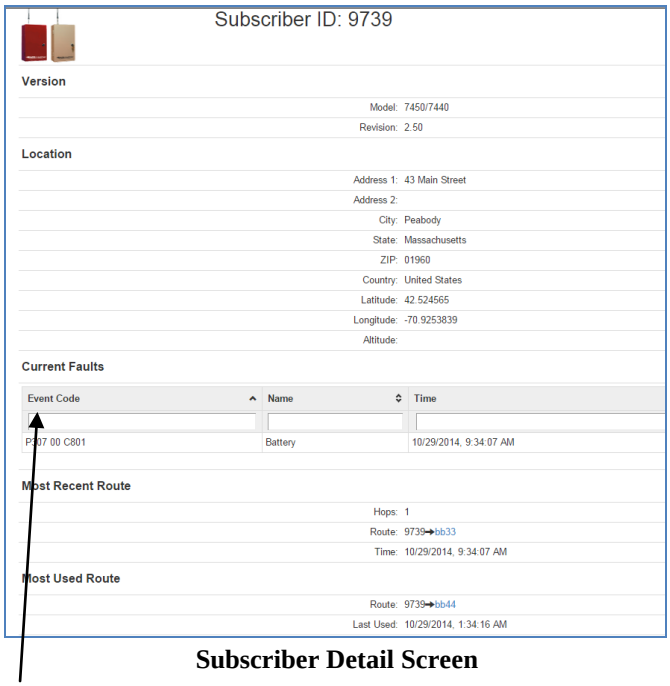

Subscriber Fault: Low Battery
Event Code: E307 00 C801
Description
Tips
Ensure that the battery is connected properly.
The battery may need to be replaced.
10 Subscribers are currently reporting this Fault
Subscriber ID
Fault Time
Address 1
Address 2
City
State
ZIP
9739 10/29/2014, 9:34:07 AM 43 Main Street Peabody Massachusetts 01960
0804 10/29/2014, 8:27:29 AM 42 West Baltimore Street Lynn Massachusetts 01902
9645 10/29/2014, 7:58:22 AM 17 Devonshire Road Middleton Massachusetts 01949
1032 10/29/2014, 7:45:12 AM 11 Dartmouth Street Malden Massachusetts 02148
6603 10/29/2014, 6:46:09 AM 32 Raynor Circle Boston Massachusetts 02120
0958 10/29/2014, 6:44:50 AM 20 Abington Road Danvers Massachusetts 01923
9682 10/29/2014, 4:22:26 AM 5 Jacobs Landing Danvers Massachusetts 01923
9683 10/29/2014, 2:40:03 AM 107 Mills Avenue Revere Massachusetts 02151
9996 10/28/2014, 5:17:04 PM 71 Howlett Street Topsfield Massachusetts 01983
Click here to automatically sort contents of any column
Enter text here to automatically search any column

Fault Detail Window

Next, single-click detail information is available for any specific Subscriber. Click on and Subscriber ID to open the **Subscriber Detail Window** that provides:

- Type of Subscriber – model and revision
- Location including address and longitude and latitude
- Current faults if any including CID codes
- Most Recent Route
- Most Used Route
- Number of repeat dependent Subscribers
- Number of generated messages over last 10 days
- Subscriber Programmed Settings
- 10 Day event history including CID codes.

Single-click detail information is also available for any specific IP Link.

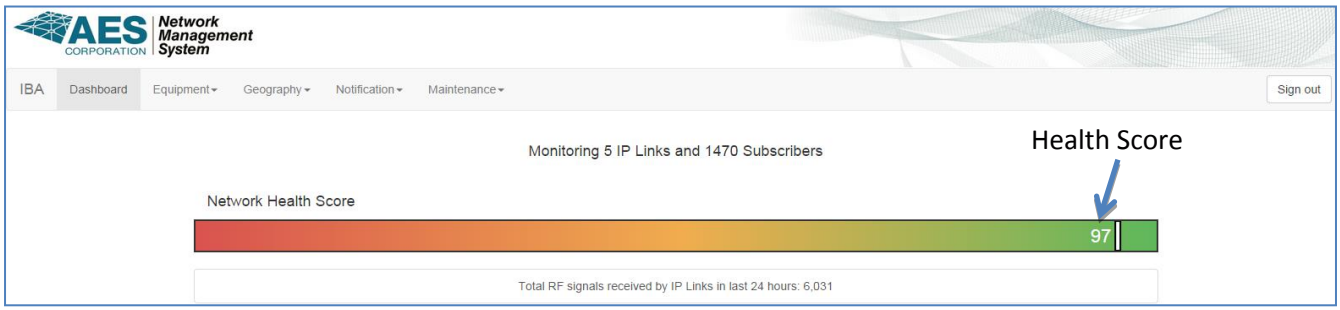


Subscriber Detail Screen

Click here to search and sort current faults

5.3 Network Health Score

The Network Health Score is a quick indicator of network performance. The score is calculated based on the number of Ack Delays, IP Link and Subscriber faults as well as the number of late check-in messages. The Health Score range is a number from 1 to 100. A higher score suggests a healthy network and a lower score suggests that improvements can be made to the network.

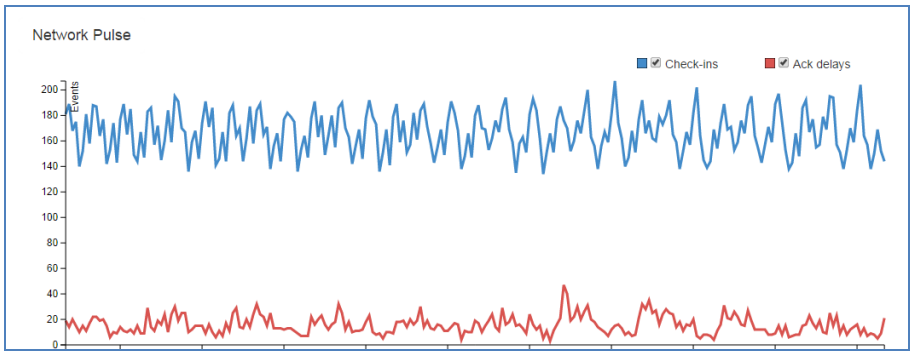


5.4 Network Pulse

The Network Pulse is a dynamic 10 day historical view of leading network health indicators. Network Pulse at the Dashboard level presents the number of Check-ins and Ack Delays in a way such that any change in network performance will be quickly visible. A consistent pattern to the Network Pulse indicates consistent network operation. If an issue develops with network performance, the number of Check-ins will decrease and the number of Ack Delays will increase. This change in performance will be quickly visible because the 10 Day pattern will change. Additional single-click detail is available by clicking on the **Network Pulse** Chart which will open a window with a 10 Day history of all events.

Network Pulse – Dashboard view
Blue line section details 10 day history of all Subscriber Check-ins

Red line section details 10 Day history of all Subscriber Ack Delays
Click on the chart to open detail view window of all events

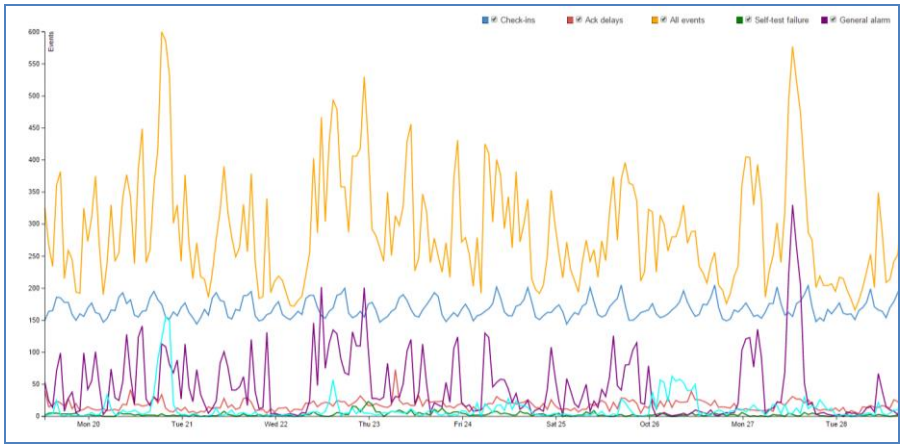


Network Pulse Dashboard View

Network Pulse – Detail view

Detail View shows a 10 day history of all events depending on check boxes at top. Includes:

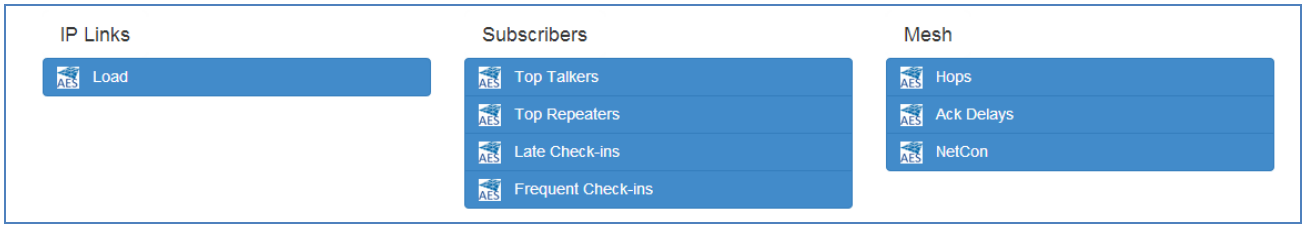
- Check-ins
- Ack Delays
- All events
- Self-test failure
- General alarm
- Fire trouble



Network Pulse Detail View

5.5 Network Analysis Tools

Under the *Network Pulse* are a set of Network Analysis tools for 3 critical network subsystem categories - IP Links, Subscribers, Mesh. Clicking down on each link opens another window which provides analytical information related to network performance. Note that these windows update automatically.



AES-*IntelliNet* Network Analysis Tools

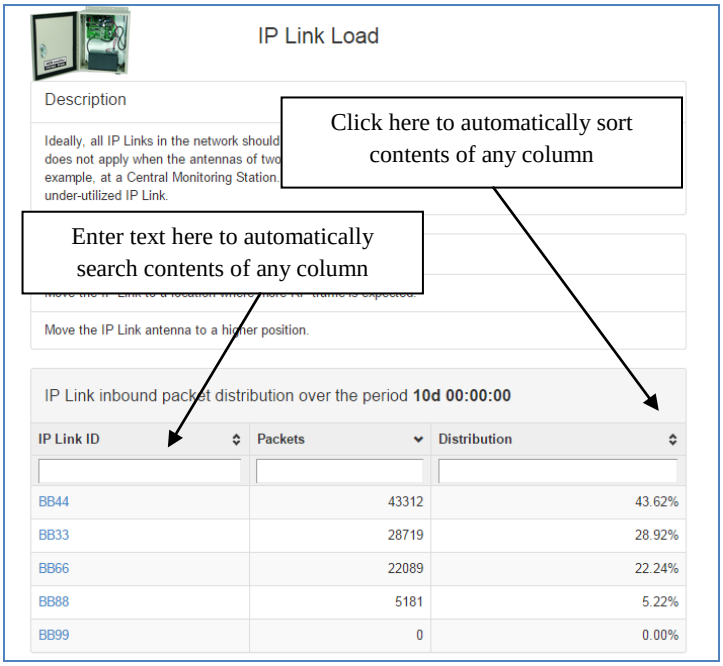
5.5.1 IP Links – Load

Click down here to see a 10 Day history of total signals and relative distribution across IP Links on the network. An example of the IP Link Load is illustrated below. Ideally, all IP Links in the network should handle roughly equal volumes of RF traffic. This generalization does not apply when the antennas of two IP Links are deliberately placed within RF range of each other such as at a Central Monitoring Station. See the Tips section describing how to increase RF traffic handled by an under-utilized IP Link.

Click on **Load** to open new window with the following information relating to the IP Links on the network:

- A description of IP Links load concept
- A number of tips are offered to generally improve network performance
- A list of the IP Links is presented at the bottom
- Additional analytical details including number of packets received by each IP Link and the distribution of packets among all of the IP Links on the network

Filters at the top of each column permit easy search and sort of the contents of the column.


IP Link Load
Description
Click here to automatically sort contents of any column
Enter text here to automatically search contents of any column
Move the IP Link antenna to a higher position.
IP Link inbound packet distribution over the period 10d 00:00:00
IP Link ID
Packets
Distribution
BB44 43312 43.62%
BB33 28719 28.92%
BB66 22089 22.24%
BB88 5181 5.22%
BB99 0 0.00%

IP Link Load

Next, single-click detail information is available for any specific IP Link. Click on any IP Link ID to open the **IP Link Detail Window** that provides:

- Version of IP Link – model and revision
- Location including address and longitude and latitude
- Current faults if any including CID codes
- Number of repeat dependent Subscribers
- Number of generated messages over last 10 days
- A section for Notes
- 10 day event history

IP Link Detail View

5.5.2 Subscribers – Top Talkers

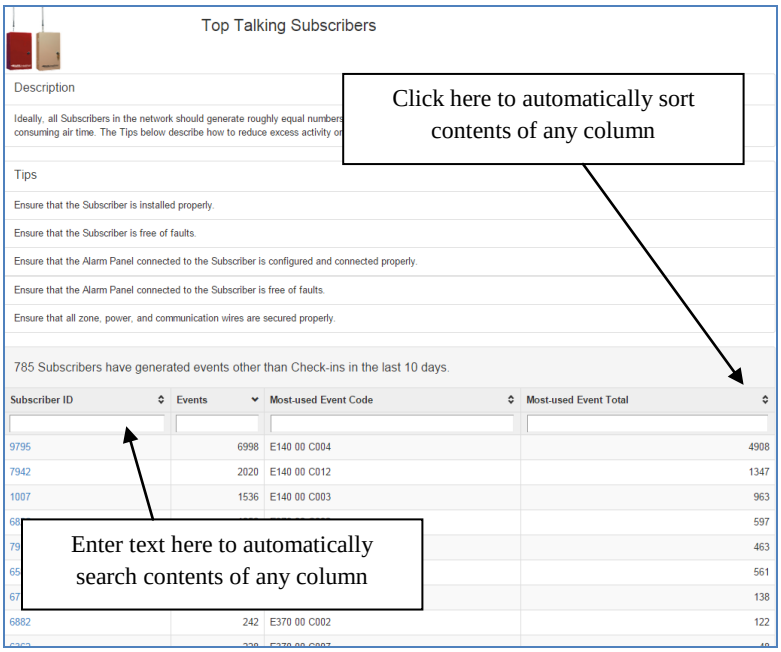
Click down here for a list of all Subscribers that have sent any signal other than Check-in during last 10 days. For each of these Subscribers, this list also includes total signals transmitted, the events most sent, and the number of times this event was sent.

Click on **Top Talkers** to open a new window with the following information relating the Subscribers on the network:

- A description of the Top Talker Concept
- Tips for generally improving network performance.
- A list of the Subscribers that generated the largest amounts of events in the last 10 days.
- The total number of events generated by each of these Subscribers
- The most used Event Code and the most used Event Code occurrence total

Filters at the top of each column permit easy search and sort of the contents of the column.

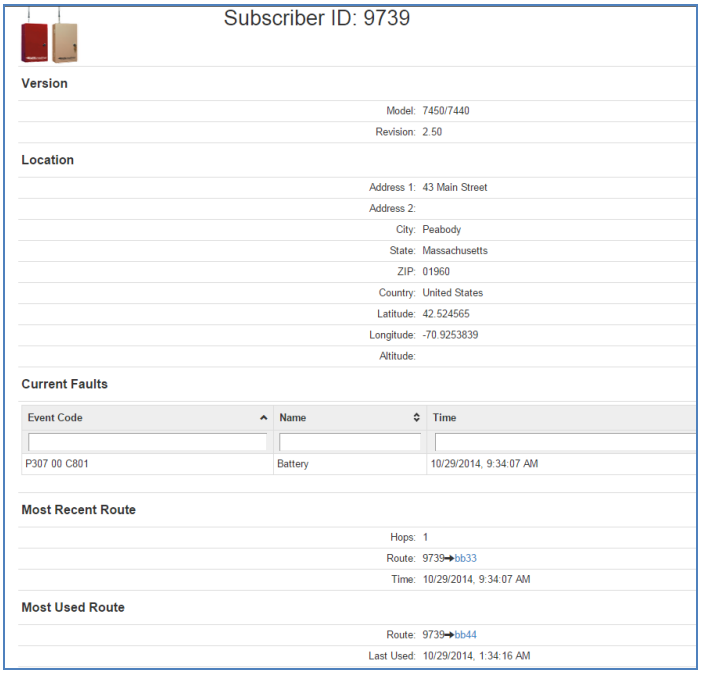
Click on any Subscriber ID to open **Subscriber Detail Window**


Top Talking Subscribers
Description
Ideally, all Subscribers in the network should generate roughly equal numbers
consuming air time. The Tips below describe how to reduce excess activity or
Click here to automatically sort contents of any column
Tips
Ensure that the Subscriber is installed properly.
Ensure that the Subscriber is free of faults.
Ensure that the Alarm Panel connected to the Subscriber is configured and connected properly.
Ensure that the Alarm Panel connected to the Subscriber is free of faults.
Ensure that all zone, power, and communication wires are secured properly.
785 Subscribers have generated events other than Check-ins in the last 10 days.
Subscriber ID
Events
Most-used Event Code
Most-used Event Total
9795 6998 E140 00 C004 4908
7942 2020 E140 00 C012 1347
1007 1536 E140 00 C003 963
597
463
561
138
6882 242 E370 00 C002 122
Enter text here to automatically search contents of any column

Top Talkers - Subscribers

Single-click detail information is available for any specific Subscriber. Click on and Subscriber ID to open the **Subscriber Detail Window** that provides:

- Type of Subscriber – model and revision
- Location including address and longitude and latitude
- Current faults if any including CID codes
- Most Recent Route
- Most Used Route
- Number of repeat dependent Subscribers
- Number of generated messages over last 10 days
- Subscriber Programmed Settings
- 10 day event history including CID codes



Subscriber Detail View

5.5.3 Subscribers – Top Repeaters

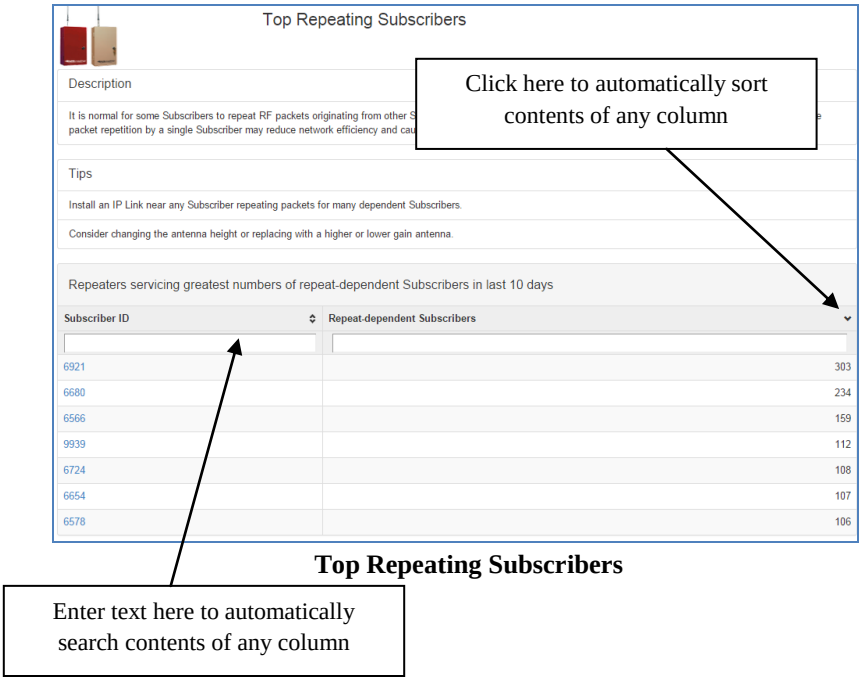
Click here for a list of Subscribers that forward the RF packets of more than 100 other Subscribers. Repeating the packets of other Subscribers is a normal function of the mesh network. Excessive packet forwarding by a single Subscriber may reduce network efficiency and cause delays though it is unlikely. It may be advisable to locate or install an additional IP Link near Subscribers forwarding RF packets from a high percentage of other Subscribers.

Click on **Top Repeaters** to open a new window with the following information relating the Subscribers on the network:

- A description of the Top Repeater Concept
- Tips for generally improving network performance.
- A list of the Subscribers that forward RF packets of more than 100 other Subscribers in past 10 days.

Filters at the top of each column permit easy search and sort of the contents of the column.

Click on any Subscriber ID to open **Subscriber Detail Window** - see section 5.5.2


Top Repeating Subscribers
Description
Click here to automatically sort contents of any column
Tips
Install an IP Link near any Subscriber repeating packets for many dependent Subscribers.
Consider changing the antenna height or replacing with a higher or lower gain antenna.
Repeaters servicing greatest numbers of repeat-dependent Subscribers in last 10 days
Subscriber ID
Repeat-dependent Subscribers
6921 303
6680 234
6566 159
9939 112
6724 108
6654 107
6578 106
Enter text here to automatically search contents of any column

Top Repeating Subscribers

5.5.4 Subscribers – Late Check-Ins

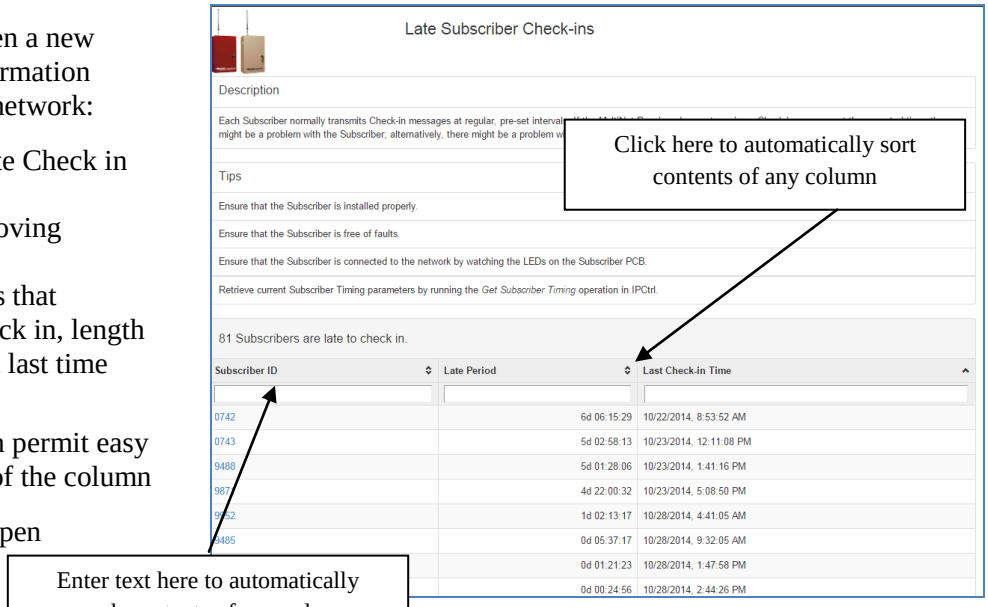
Click here for list of Subscribers from which the AES-*MultiNet* Receiver has not received a Check-in message at the expected time. This could indicate a service requirements for this Subscriber or may be explained by some environmental factor such as the weather. In order to come off this list, the Subscriber must transmit 3 Check-ins on schedule.

Click on **Late Check-ins** to open a new window with the following information relating the Subscribers on the network:

- A description of the Late Check in Concept
- Tips for generally improving network performance.
- A list of the Subscribers that currently are late to check in, length of time each is late, and last time each checked in.

Filters at the top of each column permit easy search and sort of the contents of the column

Click on any Subscriber ID to open **Subscriber Detail Window** (see Section 5.5.2)


Late Subscriber Check-ins
Description
Click here to automatically sort contents of any column
Tips
Ensure that the Subscriber is installed properly.
Ensure that the Subscriber is free of faults.
Ensure that the Subscriber is connected to the network by watching the LEDs on the Subscriber PCB.
Retrieve current Subscriber Timing parameters by running the Get Subscriber Timing operation in IPCtrl.
81 Subscribers are late to check in.
Subscriber ID
Late Period
Last Check-in Time
0742 6d 06:15:29 10/22/2014, 8:53:52 AM
0743 5d 02:58:13 10/23/2014, 12:11:08 PM
9488 5d 01:28:06 10/23/2014, 1:41:16 PM
987 4d 22:00:32 10/23/2014, 5:08:50 PM
9652 1d 02:13:17 10/28/2014, 4:41:05 AM
3485 0d 05:37:17 10/28/2014, 9:32:05 AM
0d 01:21:23 10/28/2014, 1:47:58 PM
0d 00:24:56 10/28/2014, 2:44:26 PM
Enter text here to automatically search contents of any column

Late Subscriber Check-ins

5.5.5 Subscribers – Frequent Check-Ins

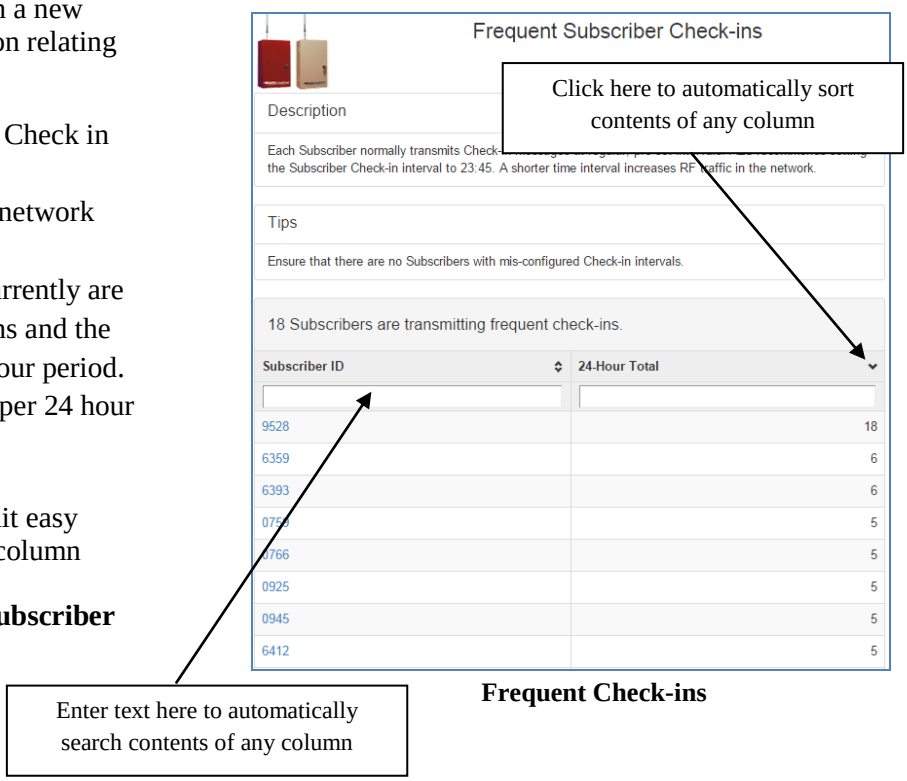
Click here for list of Subscribers transmitting more than one Check in during a 24 hour period. The list shows the number of Check ins each Subscriber transmits per 24 hour period. The recommended number of Check-ins per 24 hours is one. This meets the requirements of UL 864 for Commercial Fire and is appropriate for virtually all applications. A higher number of Check-ins per 24 hour period can unneccessarily increase RF traffic on network.

Click on **Frequent Check-ins** to open a new window with the following information relating the Subscribers on the network:

- A description of the Frequent Check in Concept
- Tips for generally improving network performance.
- List of the Subscribers that currently are transmitting frequent check-ins and the number of check-ins per 24 hour period. AES recommends 1 check in per 24 hour period.

Filters at the top of each column permit easy search and sort of the contents of the column

Click on any Subscriber ID to open **Subscriber Detail Window** - see section 5.5.2


Frequent Subscriber Check-ins
Click here to automatically sort contents of any column
Description
Each Subscriber normally transmits Check-
the Subscriber Check-in interval to 23:45. A shorter time interval increases RF traffic in the network.
Tips
Ensure that there are no Subscribers with mis-configured Check-in intervals.
18 Subscribers are transmitting frequent check-ins.
Subscriber ID
24-Hour Total
9528 18
6359 6
6393 6
0759 5
0766 5
0925 5
0945 5
6412 5
Enter text here to automatically search contents of any column

Frequent Check-ins

5.5.6 Mesh – Hops

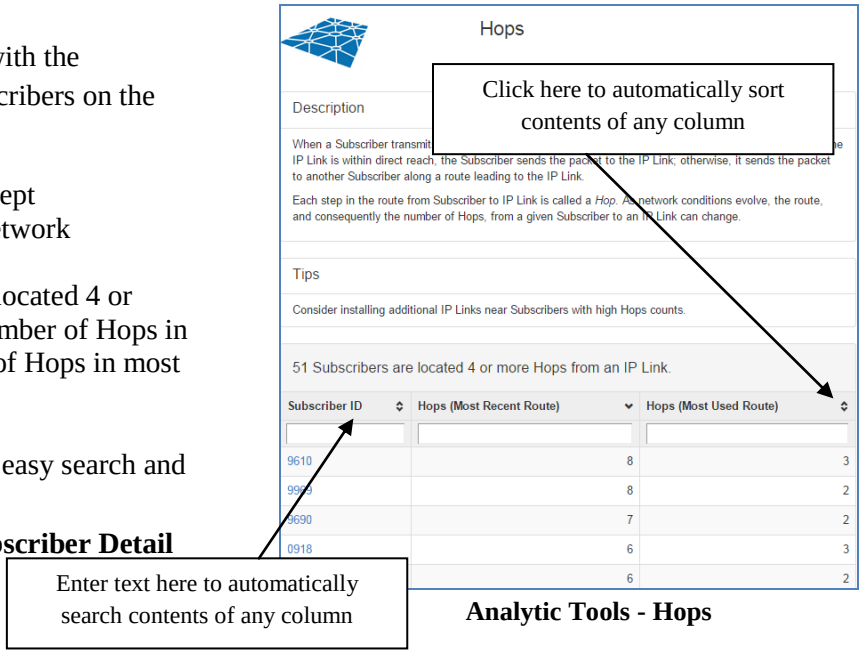
Click here for a list of Subscribers with 4 or more hops to reach an IP Link in either the most recent transmission and/or the most used route to an IP Link over the past 10 day period. It may be advisable to locate or install an additional IP Link near Subscribers on the list with 4 or more Hops.

Click on **Hops** to open a new window with the following information relating the Subscribers on the network:

- A description of the Hops Concept
- Tips for generally improving network performance.
- List of the Subscribers that are located 4 or more Hops from an IP Link, number of Hops in most recent route, and number of Hops in most used route – over past 10 days.

Filters at the top of each column permit easy search and sort of the contents of the column

Click on any Subscriber ID to open **Subscriber Detail** screen (see Section 5.5.2)


Hops
Click here to automatically sort contents of any column
Description
When a Subscriber transmit
IP Link is within direct reach, the Subscriber sends the packet to the IP Link; otherwise, it sends the packet to another Subscriber along a route leading to the IP Link.
Each step in the route from Subscriber to IP Link is called a Hop. As network conditions evolve, the route, and consequently the number of Hops, from a given Subscriber to an IP Link can change.
Tips
Consider installing additional IP Links near Subscribers with high Hops counts.
51 Subscribers are located 4 or more Hops from an IP Link.
Subscriber ID
Hops (Most Recent Route)
Hops (Most Used Route)
9610 8 3
9690 7 2
0918 6 3
6 2
Enter text here to automatically search contents of any column

Analytic Tools - Hops

5.5.7 Mesh – Ack Delays

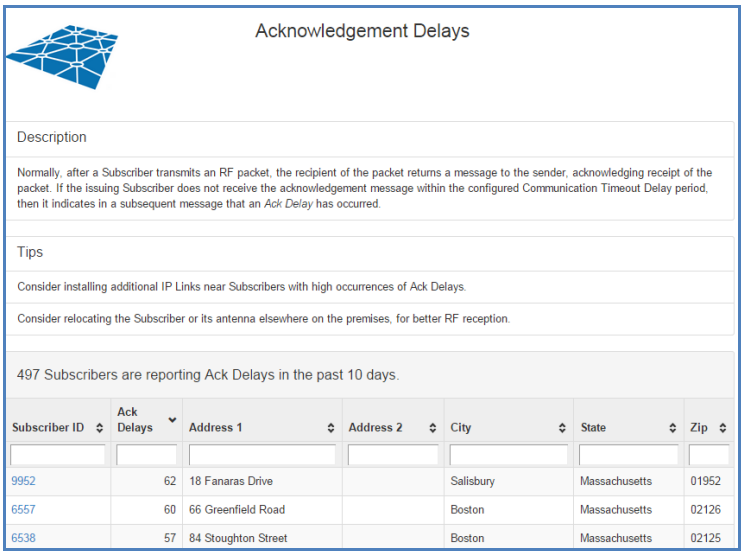
Click here for a list of all Subscribers that have transmitted an *Ack Delay* in the past 10 days as well as the quantity of *Ack Delays* over that period. When any Subscriber transmits an RF packet, the Subscriber recipient of the packet returns a message to the sender acknowledging receipt of the packet. An *Ack Delay* is triggered if a Subscriber does not receive an acknowledgement message of a transmitted signal within the configured Communication Timeout Delay period. *Ack Delays* could indicate a service requirements for a Subscriber or may be explainined by some environmental factor such as the weather. It may be advisable to locate or install additional IP Links near Subscribers that remain on the list for extended periods.

Click on **Ack delays** to open a new window with the following information relating the Subscribers on the network:

- A description of the Ack delay Concept
- Tips for generally improving network performance.
- List of the Subscribers that have reported an Ack delay over past 10 days and quantity over that period.

Filters at the top of each column permit easy search and sort of the contents of the column

Click on any Subscriber ID to open **Subscriber Detail Window** - see section 5.5.2


Acknowledgement Delays
Description
Normally, after a Subscriber transmits an RF packet, the recipient of the packet returns a message to the sender, acknowledging receipt of the packet. If the issuing Subscriber does not receive the acknowledgement message within the configured Communication Timeout Delay period, then it indicates in a subsequent message that an Ack Delay has occurred.
Tips
Consider installing additional IP Links near Subscribers with high occurrences of Ack Delays.
Consider relocating the Subscriber or its antenna elsewhere on the premises, for better RF reception.
497 Subscribers are reporting Ack Delays in the past 10 days.
Subscriber ID
Ack Delays
Address 1
Address 2
City
State
Zip
9952 62 18 Fanaras Drive Salisbury Massachusetts 01952
6557 60 66 Greenfield Road Boston Massachusetts 02126
6538 57 84 Stoughton Street Boston Massachusetts 02125

Analytic Tools - Ack delays

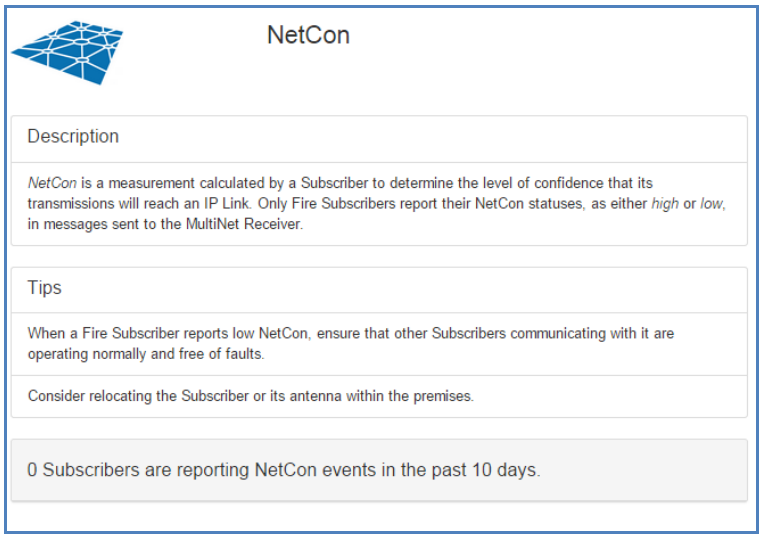
5.5.8 Mesh– NetCon

Click here for a list of all Fire Subscribers that have reported a *NetCon* fault in the last 10 days. *NetCon* is a measurement calculated by a Subscriber to determine the level of confidence that its transmissions will reach an IP Link. Only Fire Subscribers report NetCon status, as either *high* or *low*, in messages sent to the AES-*MultiNet* Receiver. When a Fire Subscriber reports low NetCon, ensure that the other Subscribers communicating with it are operating normally and are free of faults. In may be advisable to relocate the Subscriber or to relocate or change its antenna.

Click on **Netcon** to open a new window with the following information relating the Subscribers on the network:

- A description of the Netcon Concept
- Tips for generally improving network performance.
- List of the Subscribers that have reported a Netcon event over past 10 days and quantity over that period.

Click on any Subscriber ID to open **Subscriber Detail** screen (see section 5.5.2)

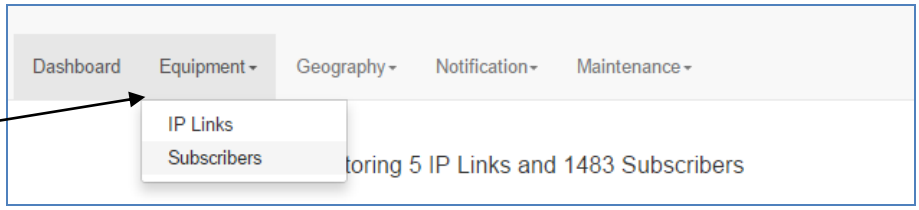

NetCon
Description
NetCon is a measurement calculated by a Subscriber to determine the level of confidence that its transmissions will reach an IP Link. Only Fire Subscribers report their NetCon statuses, as either high or low, in messages sent to the MultiNet Receiver.
Tips
When a Fire Subscriber reports low NetCon, ensure that other Subscribers communicating with it are operating normally and free of faults.
Consider relocating the Subscriber or its antenna within the premises.
0 Subscribers are reporting NetCon events in the past 10 days.

Analytic Tools - Netcon

5.6 Equipment List

Through the *Operator Dashboard*, users can obtain list of all Subscribers and all IP Links on the Business Unit Network. The Operator can sort each equipment list extensively and further click down into each Subscriber or IP Link for important information.

Click on **Equipment>IP Links**
or
Equipment>Subscribers



5.6.1 Equipment List - IP Links

A list of IP Links along with ID, Model, Revision and Location can be obtained by clicking on **Equipment** then I**P Links** at the top of the Dashboard. If IP Links are removed from the AES-*MultiNet*, they are automatically removed from this list and no longer monitored. These views can be sorted using the filters at the top of the list and can be easily printed.

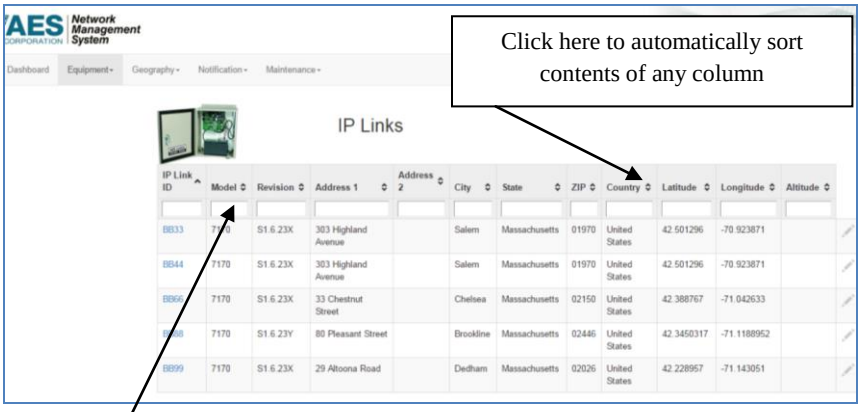
To access a list of all IP Links on a network:

Click on **Equipment>IP Links**

Information includes: IP Link ID, Model, Revision and Location

Filters at the top of each column permit easy search and sort of the contents of the column

Click on IP Link ID to open **IP Links Detail Window**


Click here to automatically sort contents of any column
IP Links
Enter text here to automatically search contents of any column

Equipment List - IP Links

Next, single-click detail information is available for any specific IP Link. Click on any IP Link ID to open the **IP Link Detail** window that provides:

- Version of IP Link – model and revision
- Location including address and longitude and latitude
- Current faults if any including CID codes
- Number of repeat dependent Subscribers
- Number of generated messages over last 10 days
- A section for Notes
- 10 Day searchable and sortable event history

IP Link Detail View

5.6.2 Equipment List - Subscribers

A list of Subscribers along with ID, Model, Revision and Location can be obtained by clicking on **Equipment** then **Subscribers** at the top of the Dashboard. If Subscribers are removed from the AES-*MultiNet*, they are automatically removed from this list and no longer monitored. These views can be sorted using the filters at the top of the list and easily printed.

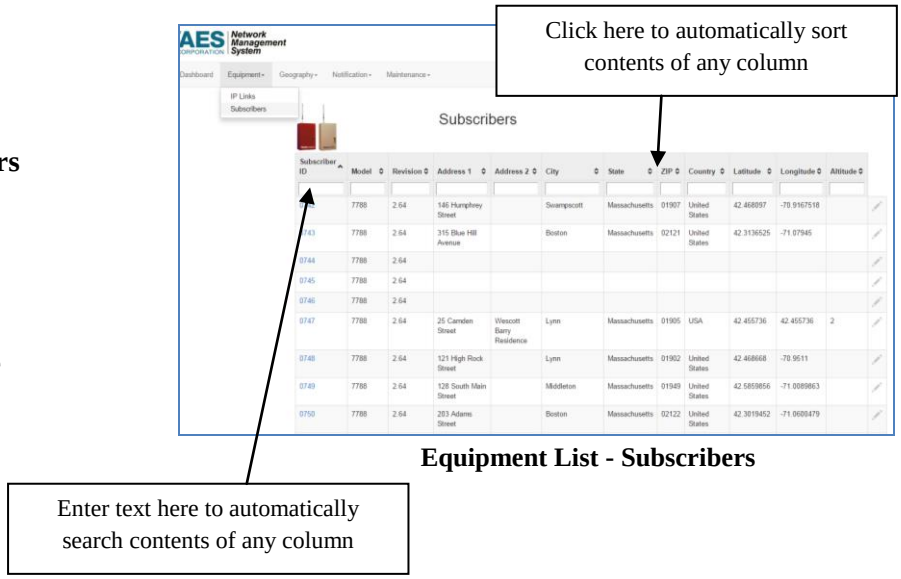
To access a list of all Subscribers on a network:

Click on **Equipment>Subscribers**

Information includes: ID, Model, Revision and Location

Filters at the top of each column permit easy search and sort of the contents of the column

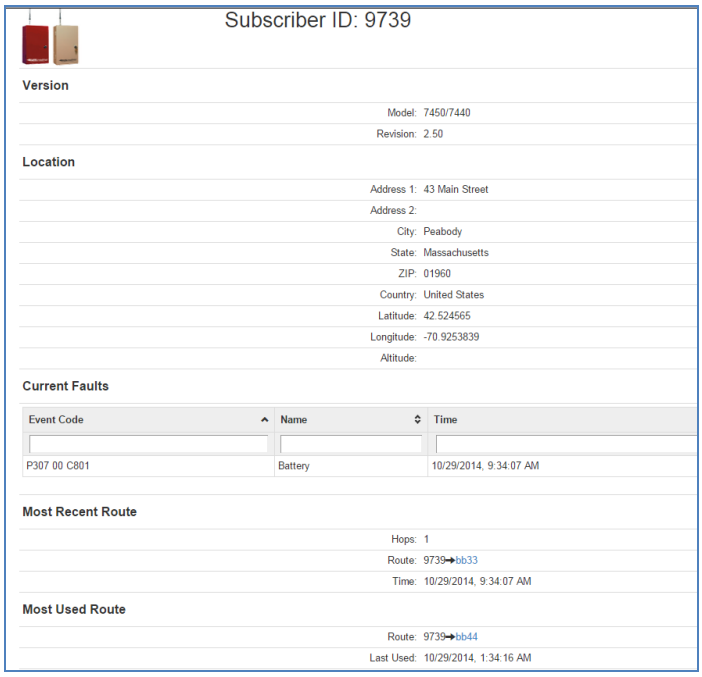
Click on Subscriber ID to open **Subscriber Detail Window**


Click here to automatically sort contents of any column
Subscribers
Enter text here to automatically search contents of any column

Equipment List - Subscribers

Single-click detail information is available for any specific Subscriber. Click on and Subscriber ID to open the **Subscriber Detail Window** that provides:

- Type of Subscriber – model and revision
- Location including address and longitude and latitude
- Current faults if any including CID codes
- Most Recent Route
- Most Used Route
- Number of repeat dependent Subscribers
- Number of generated messages over last 10 days
- Subscriber Programmed Settings
- 10 Day searchable and sortable event history including CID codes

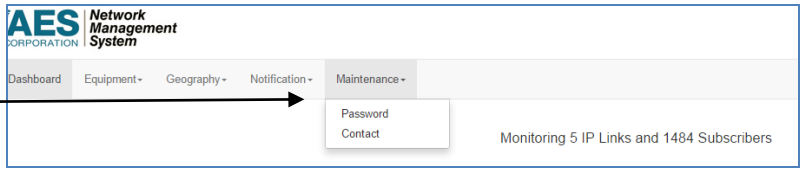


Subscriber Detail View

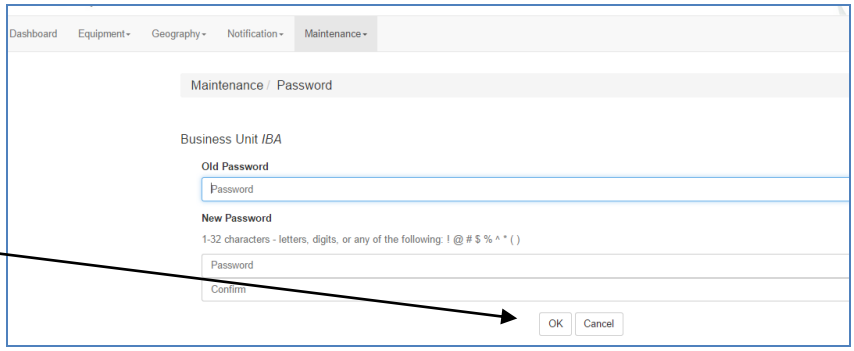
5.7 Maintenance – Operator Dashboard

Through the Maintenance dropdown on the *Operator Dashboard*, users can easily change the Business Unit password and contact information.

To change the Password, click on **Maintenance > Password** to launch the screen below

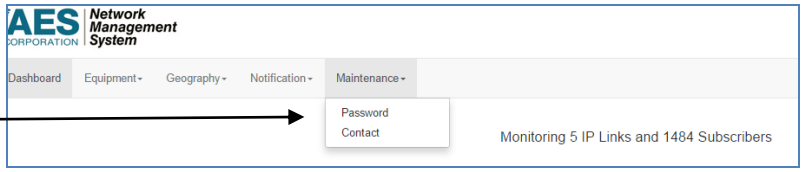


First, enter the current password and then the new password twice .
Click **OK** to save the new password.

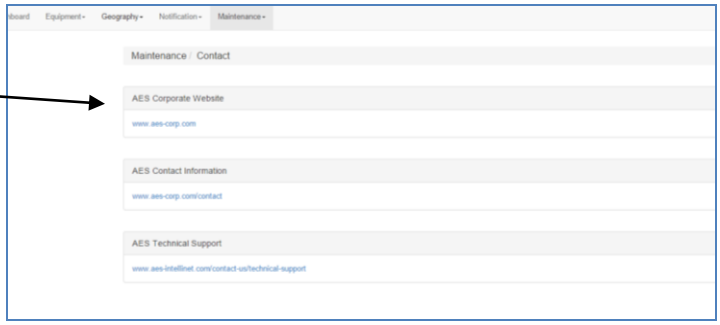


To change the Business Units Contact Information, click on **Maintenance > Contact** to launch the screen below:

To change the contact information
Click on **Maintenance > Contact** to launch the screen below



Enter or change contact information.



6 Interactive Visualization

6.1 Overview

Through the NMS *Operator Dashboard*, a user can launch an interactive satellite map of their AES-*IntelliNet* network that uses Google Earth™. The map shows the location and status of all IP Links and Subscribers and illustrates the multiple routes for RF signals across the network from each Subscriber over past 10 days.

All interactive satellite maps are refreshed automatically as new data is received. By clicking in any IP Link or Subscriber icon, the following information is accessible: ID, Version, Settings, Location, Current Faults, Communication Trends, editable Notes and Event History. By providing a comprehensive visualization of the network and its subsystems, the network map helps with planning for network expansion. There are four discrete views the user can access for interactive visualization of their network. The four network views are **Utilization, Routes, Faults, and Topology**. Sections 6.4 through 6.7 explain each of the four network views.

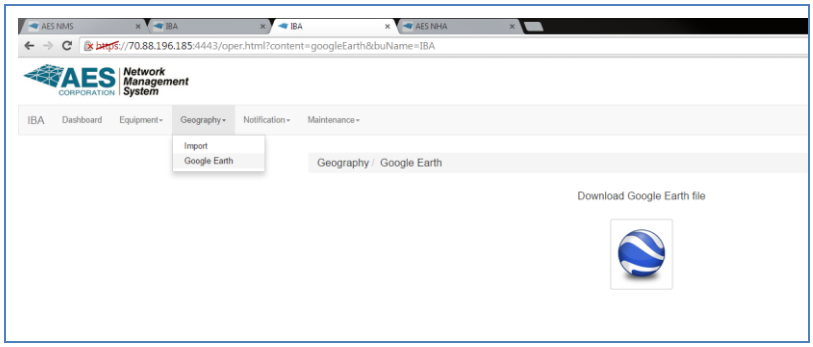
In order to view the visualization feature of NMS, Google Earth (https://www.google.com/earth/) must be installed on the PC you plan to use.

6.2 Enter Subscriber and IP Link Addresses into NMS

In order to view the Visualization feature of the NMS on Google Earth you have to first load the addresses of the Subscribers and IP Links. To import the street addresses go to **Geography** then **Import**. You can download a template which can be used to import all the addresses. After the addresses are imported, the NMS server will resolve to latitude and longitude and display progress.

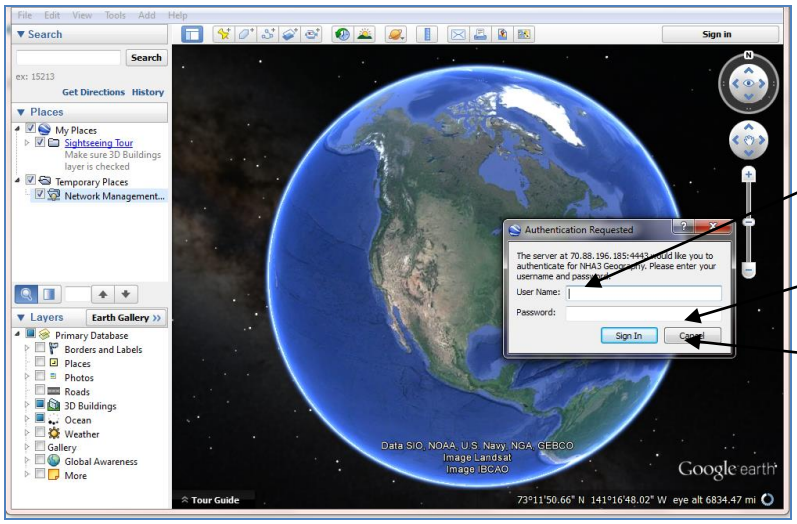
6.3 Launch Interactive Visualization

To launch the Visualization function, click on **Geography>Google Earth** to view the screen below



Click on the Google Earth icon to download the .klm file with the Business Unit map information. The Business Unit .klm file will download an icon to the bottom left of the screen.

Next click on he Business Unit .klm file. As Google Earth begins to launch, you will be asked to enter a User Name and password. The user name is the name of the Business Unit and the password is the same used for the *Operator Dashboard* password for that Business Unit. Next, enter user name and password and click **Sign In.**

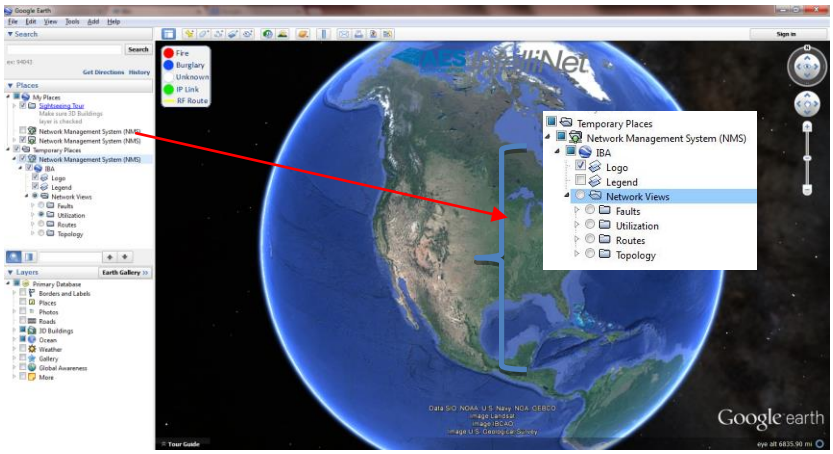


Enter the name of the Business Unit as the User Name and

Use *Operator Dashboard* password

Click **Sign In.**

After clicking on **Sign In**, the Business Unit data base will load which could take a few minutes.



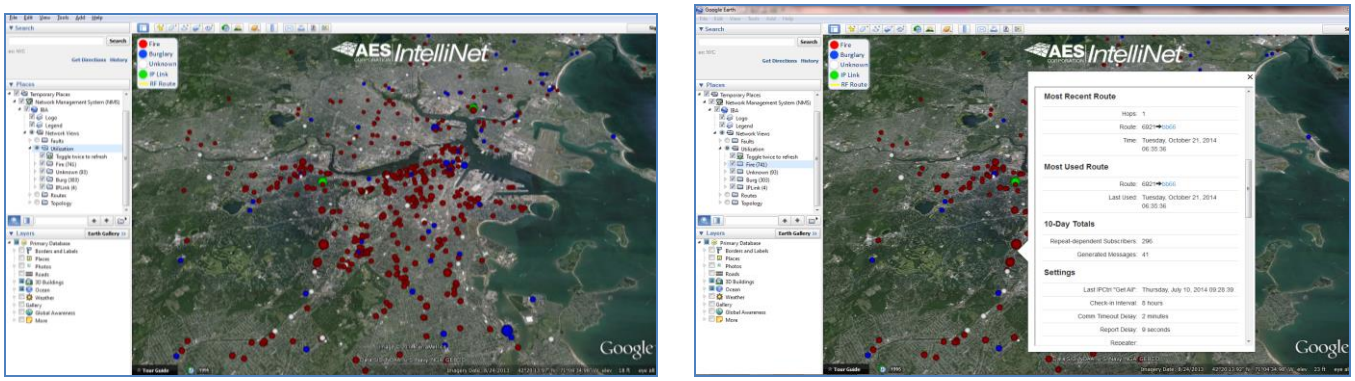
On the left of the screen will be the NMS Google Earth Summary as detailed above. At the top of the Summary under AES-*Network Management System* is the name of the Business Unit – in this example the Business Unit name is IBA. Below the Business Unit name are check boxes that control whether the Legend and the AES-*IntelliNet* logo are visible on screen. Note in the Legend that the AES Fire Subscribers are red, Burglary Subscribers are blue, and unknown Subscribers are white.

Next in the Google Earth Summary are the four Network views which present the interactive maps of the AES-*IntelliNet* network from four different perspectives. The four network views are **Utilization, Routes, Faults, and Topology**. Sections 6.4 through 6.7 explain each of the Four Network Views.

Next, double click on the **Utilization** view to populate the map with the Subscribers and IP Links from this Business Unit network. The program will zoom into the network geography.

6.4 Utilization View

This view provides an interactive satellite map that highlights the most often used Subscribers for signal delivery across the network to IP Links. The graphical size of the Subscriber icon on the map illustrates relative utilization of each Subscriber as measured by the number of repeat dependent Subscribers.

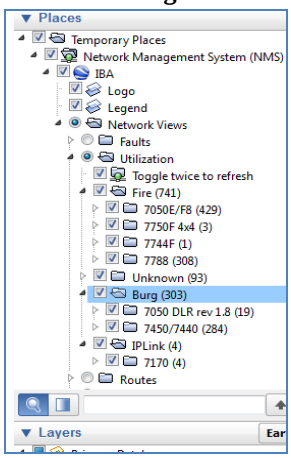


Utilization View - The larger the Subscriber icon indicates a higher number of repeat dependent Subscribers

Single-click detailed information is available for all Subscribers. Click on any Subscriber icon to get a view of the following real time information: Type of Subscriber – model and revision, location including address and longitude and latitude, current faults if any including CID codes, Most Recent Route, Most Used Route, number of repeat dependent Subscribers and number of generated messages over last 10 days, Subscriber Programmed Settings, and a 10 day event history including CID codes.

The components of the network detailed on the interactive map can be modified using the Google Earth Summary. Expanding the check boxes below the **Utilization** view enables users to select, and limit if needed, the Subscribers and IP Links that are displayed based on Subscriber type and Subscriber model.

Utilization View – Google Earth Summary

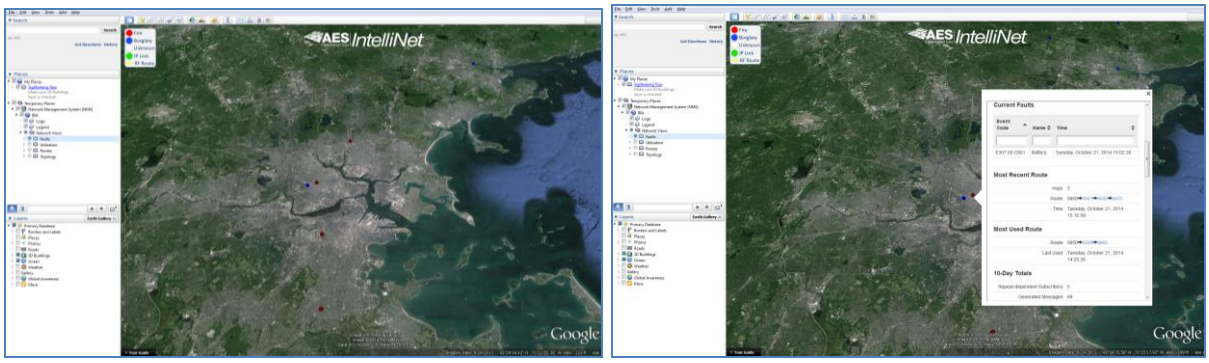


Users can select Subscribers and IP Links to view on the interactive map using Google Earth Summary

The value of the Utilization view for managing an *IntelliNet* Network is that it can identify potential network bottlenecks to enable proactive network management for optimal performance. To return to the Utilization view, double click on **Utilization** in the Google Earth Summary.

6.5 Faults View

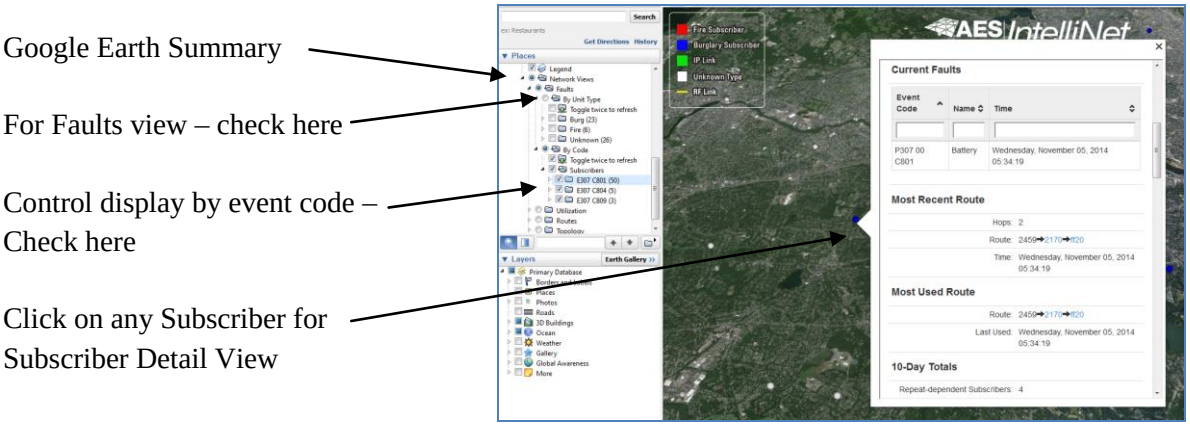
This view provides an interactive satellite map of all subscribers with a current fault condition. Subscribers with a new fault will automatically appear on the map. When a fault restores, the Subscriber will disappear from this view. To access the Faults view, double click on **Faults** in the Google Earth Summary.



Faults View - User can display Subscribers with a current fault real time and click down for details to plan service

Single-click detailed information is available for all Subscribers in the Fault view. Click on any Subscriber icon to get information on the current fault and a view of the following real time information: Type of Subscriber – model and revision, location including address and longitude and latitude, current fault CID codes, Most Recent Route, Most Used Route, number of repeat dependent Subscribers and number of generated messages over last 10 days, Subscriber Program Settings, and a 10 Day event history including CID codes.

The Subscribers with a fault that are detailed on the interactive map can be modified using the Google Earth Summary. Expanding the check boxes below the **Faults** view enables users to select, and limit if needed, the Subscribers with a fault that are displayed based on Subscriber type, Subscriber model, or by event code. For example the illustration below details Subscribers with a fault sorted by event code - see the Google Earth Summary check boxes.

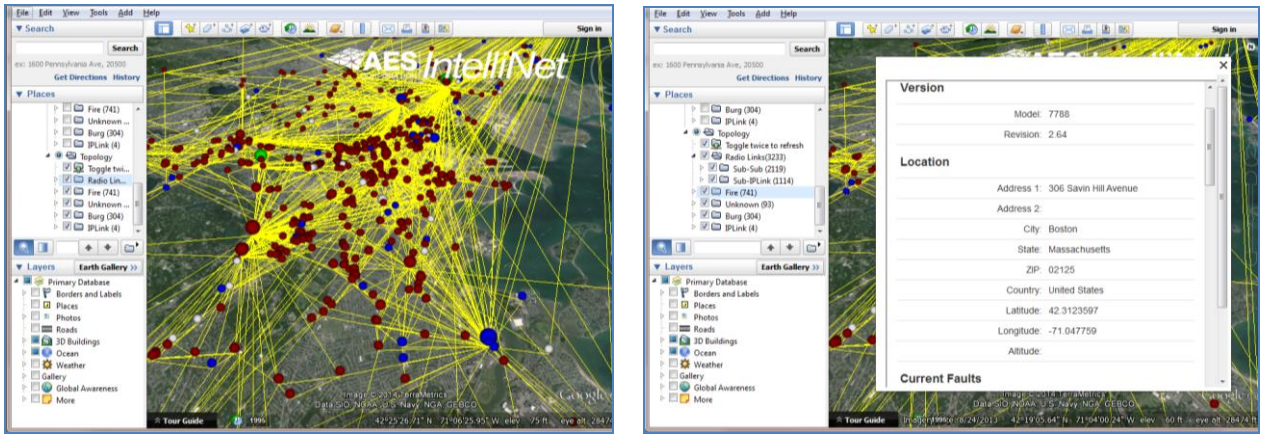

Google Earth Summary
For Faults view – check here
Control display by event code – Check here
Click on any Subscriber for Subscriber Detail View
AES IntelliNet
Current Faults
Most Recent Route
Most Used Route
10-Day Totals

Users can select Subscribers to view by type and model or event code

The value of the **Faults** view is that it can simplify planning for routine service of Subscribers so that it can be scheduled cost effectively within normal workflows.

6.6 Mesh Topology View

This view provides an interactive satellite map of all Subscribers and illustrates on the map the RF paths between each Subscriber and the IP Links. In additional to detailed Subscriber information, user can click on any path and obtain RF Link data including the beginning and end nodes and the distance between the nodes.



Topology View - User can display RF paths between Subscribers and IP Links

Single-click detailed information is available for all Subscribers in the Topology view. Click on any Subscriber icon to get a view of the following real time information: Type of Subscriber – model and revision, location including address and longitude and latitude, current faults if any including CID codes, Most Recent Route, Most Used Route, number of repeat dependent Subscribers and number of generated messages over last 10 days, Subscriber Program Settings, and a 10 Day event history including CID codes.

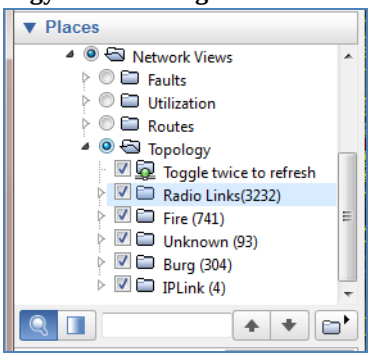
Single-click information is also available on any of the RF paths between Subscribers and IP Links illustrated on the map. Click on a line representing an RF path to create a pop up box with the details of that particular RF Link that includes the distance of the link and ID of the beginning and end nodes of the link.

.

User can access the details of any RF path on the network

The components of the network detailed on the interactive map can be modified using the Google Earth Summary. Expanding the check boxes below the **Topology** view enables users to select, and limit if needed, the Subscribers and IP Links that are displayed on the map based on Subscriber type and Subscriber model.

Topology View – Google Earth Summary

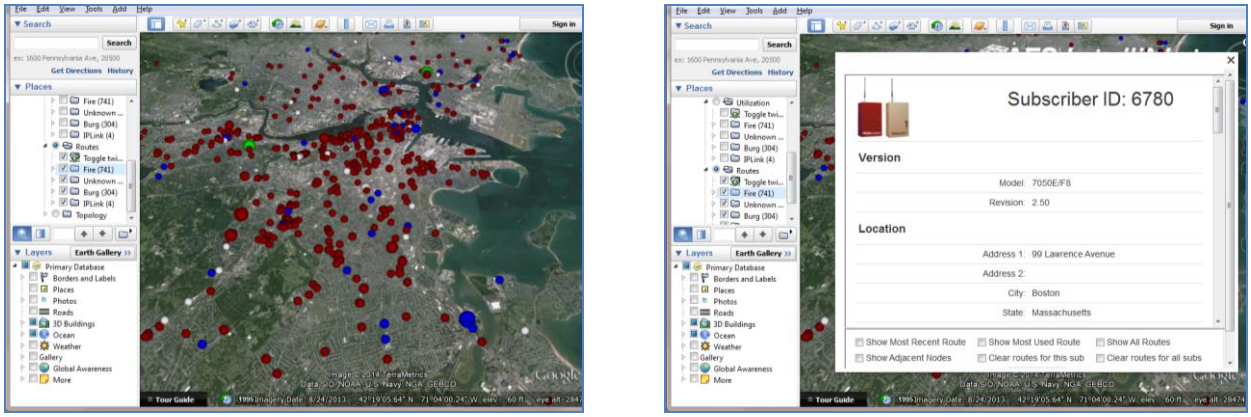


Users can select Subscribers to view by type and model

The value of the **Topology** view is that it is a powerful tool for planning network growth – detailing optimal locations for new Subscribers and the basis for planning expansion into new geographies.

6.7 Routes View

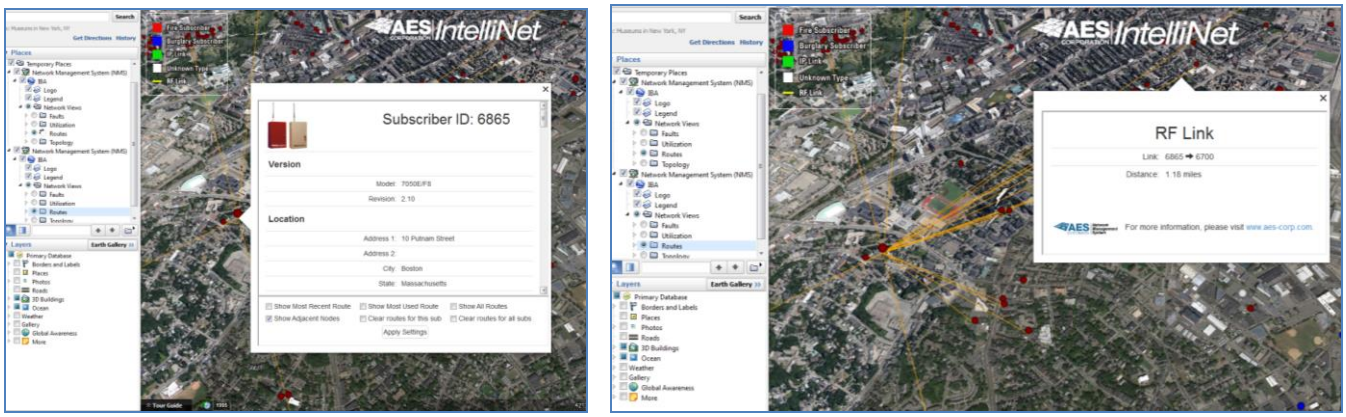
This view provides an interactive satellite map that enables users to view the historical RF paths, or routes, between Subscribers and other Subscribers, and Subscribers and IP Links over the past 10 day period. It shows route information on the map that includes most recent route, most used route, as well as details on adjacent nodes and peers. To access the Routes view, double click on **Routes** in the Google Earth Summary.



Routes View - Users can access historical RF path information for any Subscriber

Single-click detailed information is available for all Subscribers in the Routes view. Click on any Subscriber icon to enable interactive access to route information. Use the check boxes at the bottom to generate specific route information on the map. This information includes most recent route, most used route, all routes used, and to identify adjacent nodes. Below is an example of detailed information generated in Visualization to identify the adjacent nodes for a Subscriber on the network.

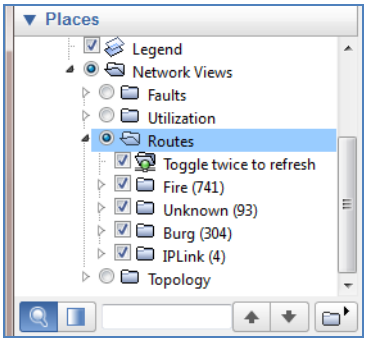
Routes View - Identifying Adjacent Nodes



Click on **Show Adjacent Nodes** and then click **Apply Settings** to illustrate on map all other Subscribers with which this Subscriber has exchanged RF communication in the past 10 days. Single-click information is available for the RF paths illustrated on the map. Click on a line representing an RF path to create a pop up box (see above) with the details of that particular RF Link that includes the distance of the link and ID of the beginning and end nodes.

The components of the network detailed on the interactive map can be modified using the Google Earth Summary. Expanding the check boxes below the **Routes** view enables users to select, and limit if needed, the Subscribers that are displayed based on Subscriber type and Subscriber model.

Routes View – Google Earth Summary



Users can select Subscribers to view on the interactive map by type and model

7 Notification

7.1 Notification Set-up

The Notification function enables users to monitor their AES-*IntelliNet* network from anyplace at any time. Through the *Operator Dashboard*, users can configure automatic alerts based on a change to the *Network Health Score* or a fault with any Subscriber or IP Links. Separate drop down menus enable the user to easily create the list of personnel to be notified by both SMS and email, define the fault criteria to be reported, and create associations between the alert triggers and personnel to optimize response.

Set up Notifications

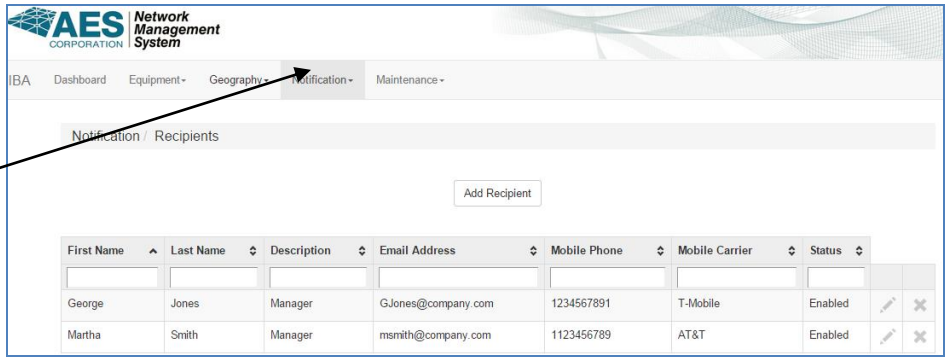
In order to set up and manage the Notification function, click on **Notification** and then on each of the following sections:

- **Recipients** – To identify personnel that receive one or more alerts
- **Triggers** – To define network events from which to generate alerts
- **Associations** – To map personnel or recipients to trigger events

7.2 Recipients

To add personnel to the alert list or to edit information about an existing Recipients, change the status of a Recipient, or delete a Recipient, click on **Notification > Recipients** to launch the screen below.

Click on
Notifications > Recipients



Recipient View

To edit an existing Recipient, click on the pencil icon to bring up the Edit Recipient screen. In this screen you can also change the status of a Recipient from Enabled to Disabled. SEE NEXT PAGE.

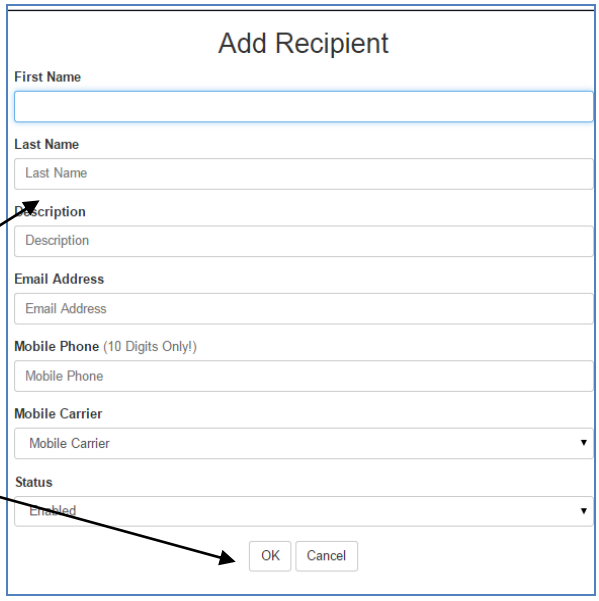
To delete a Recipient, click on the X icon to the far right. You will be asked to CONFIRM that you want to delete the Recipient.

To add a new Recipient, click on **Add Recipient** button at top. SEE NEXT PAGE.

To add a new Recipient, click on **Add Recipient** button at top of Recipient view

Input contact information including email address and mobile phone number

Click **OK** to complete and save the Recipient information**.**

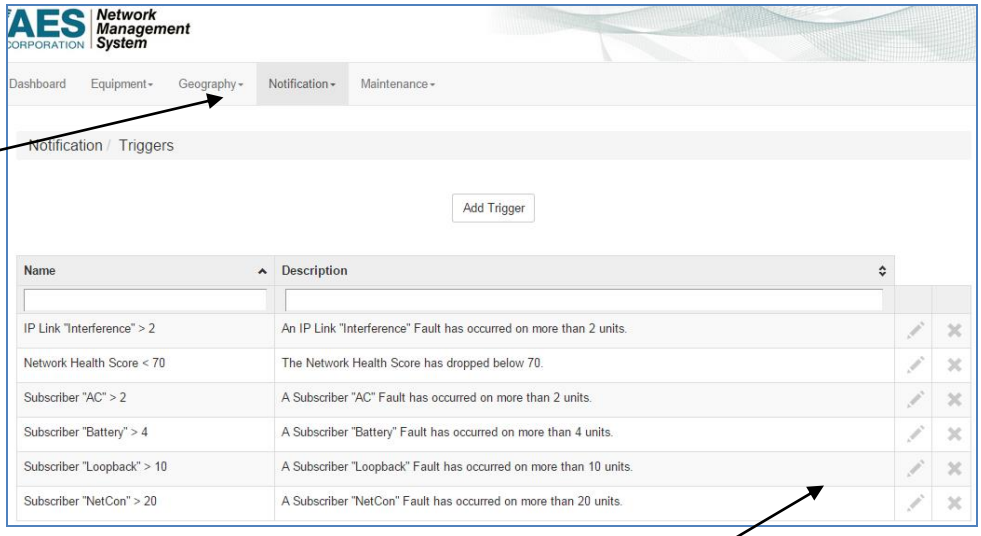


Add Recipient View

7.3 Triggers

To add a network events that will trigger an alert, click on **Notification >Triggers** to launch the Manager Triggers screen below - In this screen you can also edit or delete an existing Trigger.

Click on
Notifications > Triggers



Manage Triggers Screen

To edit an existing Trigger, click on the pencil icon to bring up the Edit Trigger screen.

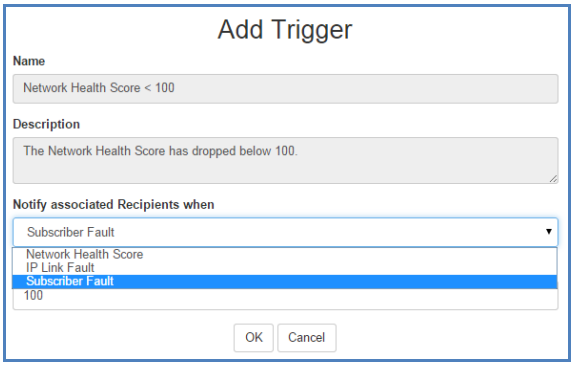
To delete a Trigger, click on the X icon to the far right. You will be asked to CONFIRM that you want to delete the Trigger.

To add a new Trigger, click on **Add Trigger** button at top. SEE NEXT PAGE

To add a new Trigger, click on **Add Trigger** button at top of Manage Triggers Screen

There are three criteria for triggers – see below.

Click **OK**
to complete and save the Trigger information**.**



Add Trigger View

There are three criteria for each alert Trigger event defined.

- Fault source – there are 3 possible fault sources – (1) a reduction in the Network Health Score below a set score, (2) an IP Link Fault, and (3) Subscriber Fault
- Fault type – These are defined in the drop down lists for Subscriber Fault and IP Link Fault
- Minimum events needed to alert – the number of occurrences requires to send the alert

Input your selections from the three criteria above then click **OK** to complete and save the Trigger**.**

7.4 Associations

To map Recipients to Triggers, click on **Notification > Associations** to launch the screen(s) below - In these screens you can view list of recipients and associated Triggers or a list of Triggers and associated Recipients depending which 'view by' box is checked at the top of the screen.

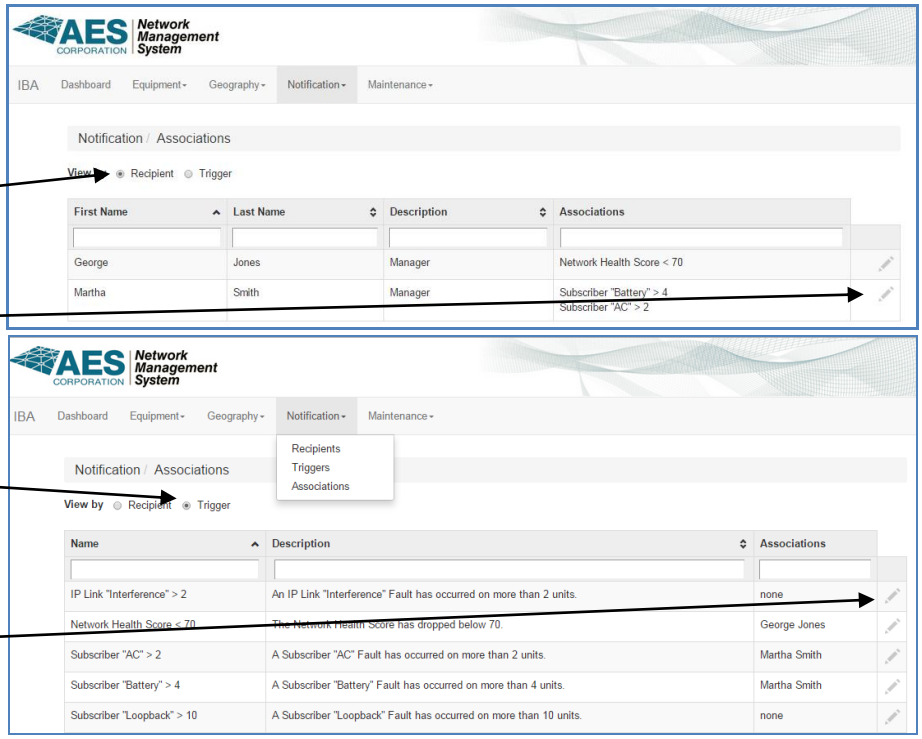
Click on **Notification > Associations**

Sorted by Recipients and associated Triggers

To add or edit an association Click on the pencil icon

Sorted by Triggers and associated Recipients

To add or edit an association Click on the pencil icon

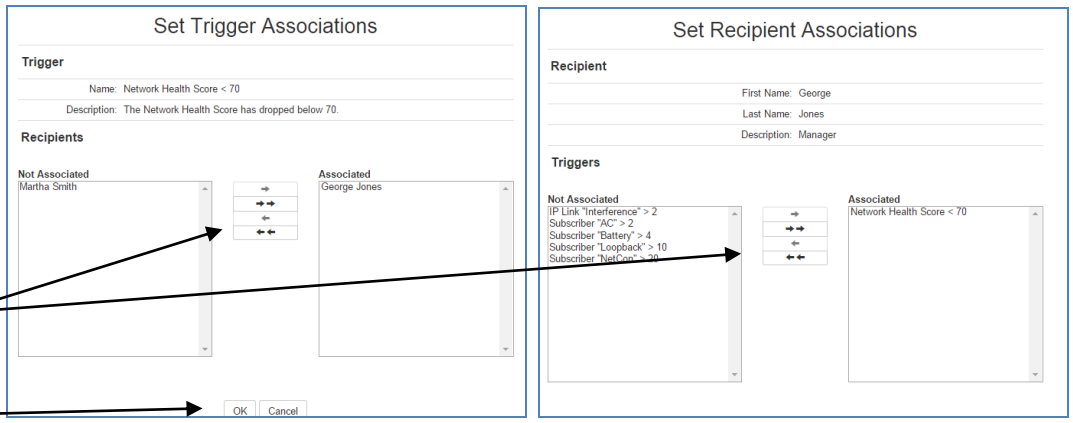


To set a new Association or edit an existing Association, click on the pencil icon on the right of the grid. See screens below. Use arrows as needed to manage Associations and click on **OK** to save.

Set a new or edit an existing Association

Use arrows to adjust Associations

Click **OK**



NOTE: If a notification has been already sent out to existing recipients, all new recipients added after this notification will not receive notifications until the status of the associated triggers drops below the threshold. Only after the trigger status is below the threshold will the new and existing recipients receive notifications when the threshold is surpassed.

8 Warranty

OWNER WARRANTY - AES CORPORATION
LIMITED PRODUCT WARRANTY AND TECHNOLOGY LICENSE

LIMITED PRODUCT WARRANTY:
AES Corporation ("AES") warrants to the original purchaser that each AES Subscriber Product will be free from defects in material and workmanship for three (3) years from date of purchase and all other products purchased from AES including central station receivers and accessories will be warranted for one (1) year from the date of purchase. At no cost to the original purchaser for parts or labor, AES will repair or replace any AES Product or any, part or parts thereof which are judged defective under the terms of this Warranty.

Defective AES Products must be returned to AES directly, provided they are properly packed, postage prepaid. Or exchange may be made through any authorized direct factory representative for any AES Products that are judged defective under the terms of this Warranty. Improper or incorrectly performed maintenance or repair voids this Warranty. This Warranty does not cover replacement parts that are not approved by AES. This Warranty does not apply to any AES Product or any part thereof that has been altered in any way to affect its stability or reliability, or that has been subjected to abuse, misuse, negligence, accident or act of God, or that has had the serial number effaced or removed.

Certain AES *Products* are designed to operate and communicate with other specified AES Products and certain other specified products, systems or networks authorized or approved by AES, as identified in the applicable AES Product instructions. This Warranty does not apply to any AES Product that is used with any unauthorized or unapproved products, systems or networks, or that has been installed, applied or used in any manner, other than in strict accordance with AES instructions.

AES makes no warranty, express or implied, other than what is expressly stated in this Warranty. If the law of your state provides that an implied warranty of merchantability, or an implied warranty of fitness for particular purpose, or any other implied warranty, applies to AES, then any such implied warranty is limited to the duration of this Warranty.

AES cannot be aware of and is not responsible for the differing values of any property to be protected by its alarm reporting systems. This Warranty does not cover and AES shall not be liable for any defect, incidental or consequential, loss or damage arising out of the failure of any AES Product to operate.

Some states do not allow the exclusion or limitation of the durations of implied warranties or the limitation on incidental or consequential damages, so the above limitations or exclusions may not apply to you.

This Warranty gives you specific legal rights and you may also have other rights that vary from state to state.

TECHNOLOGY LICENSE:
Certain AES Products include software, protocols and other proprietary and confidential technology and trade secrets of AES which are incorporated in or provided with AES Products solely for use in conjunction with and in order to operate AES Products ("Licensed Technology"). AES grants the original purchaser a non-exclusive license to use such Licensed Technology solely in connection with the use and operation of AES Products and for no other purpose or use whatsoever. No title or ownership in or to any such Licensed Technology is conveyed by the sale or delivery of any AES Products; all such rights are retained by AES.

AES SERVICE PROCEDURE: Contact AES by phone (978) 535-7310, fax (978) 535-7313, or email Julie Hickey at jhickey@aes-intellinet.com to receive a Return Material Authorization (RMA) number. Please have the AES part number and serial number ready. Repack equipment in original or equivalent packaging. Inside the box, include contact name, telephone number, address, and a brief description of the reason for return.

Ship items freight-prepaid to:
Repair Services, RMA#_____
AES Corporation
285 Newbury Street
Peabody, MA 01960 USA
(Contact AES for Return Material Authorization number)

November 2014